# BSc Year 2 – Data Communications Lab - Using Wireshark to View Network Traffic

# Topology



# **Objectives**

## Part 1: (Optional) Download and Install Wireshark

## Part 2: Capture and Analyze Local ICMP Data in Wireshark

- Start and stop data capture of ping traffic to local hosts.
- Locate the IP and MAC address information in captured PDUs.

#### Part 3: Capture and Analyze Remote ICMP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IP and MAC address information in captured PDUs.
- Explain why MAC addresses for remote hosts are different than the MAC addresses of local hosts.

# Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

#### **Required Resources**

- 1 PC (Windows 7or 8, Vista, or XP with Internet access)
- Additional PC(s) on a local-area network (LAN) will be used to reply to ping requests.

# Part 1: (Optional) Download and Install Wireshark

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In Part 1 of this lab, you will download and install the Wireshark software program on your PC.

Note: If Wireshark is already installed on your PC, you can skip Part 1 and go directly to Part 2.

#### Step 1: Download Wireshark.

- a. Wireshark can be downloaded from www.wireshark.org.
- b. Click Download Wireshark.



c. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

#### Step 2: Install Wireshark.

- a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.
- Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click Yes to uninstall the previous version of Wireshark.



c. If this is the first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.



d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

🐼 Wireshark 1.8.3 (64-bit) Setup	
License Agreement Please review the license terms before installing Wireshark 1.8.3 (64-bit).	
Press Page Down to see the rest of the agreement.	
This text consists of three parts: Part I: Some remarks regarding the license given in Part II: The actual license that covers Wireshark. Part III: Other applicable licenses. When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.	
If you accept the terms of the agreement, dick I Agree to continue. You mus agreement to install Wireshark 1.8.3 (64-bit).	₹ st accept the
Nullsoft Install System v2.46 — Sack I Agree	Cancel

e. Keep the default settings on the Choose Components window and click Next.

🛃 Wireshark 1.8.3 (64-bit) Setup	)	
Choose Components Choose which features of Wires	hark 1.8.3 (64-bit) you want to install.	
The following components are a	vailable for installation.	
Select components to install:	<ul> <li>✓ Wireshark</li> <li>✓ TShark</li> <li>✓ Plugins / Extensions</li> <li>✓ Tools</li> <li>✓ User's Guide</li> </ul>	
Space required: 102.4MB	Description Position your mouse over a component to see description.	; its
Nullsoft Install System v2,46	< Back Next >	Cancel

f. Choose your desired shortcut options and click Next.

Wireshark 1.8.3 (64-bit) Setup	
Select Additional Tasks Which additional tasks should be done?	
Create Shortcuts  Start Menu Item  Desktop Icon  Quick Launch Icon  File Extensions  Associate trace file extensions to Wireshark (5vw, acp, apc, atc, cap, enc, erf, fdc, pcap, pcapng, pkt, snoop, syc, tpc, tr1, trace	, bfr, e, trc, wpc, wpz,
Nullsoft Install System v2.46 ————————————————————————————————————	t > Cancel

g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.

🐼 Wireshark 1.8.3 (64-bit) Setup	
<b>Choose Install Location</b> Choose the folder in which to install Wireshark 1.8.3 (64-bit).	
Choose a directory in which to install Wireshark.	
Destination Folder	
C:\Program Files\Wireshark	Browse
Space required: 102.4MB Space available: 81.5GB	
Nullsoft Install System v2.46	Next > Cancel

- h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommend that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.
- i. Finish the WinPcap Setup Wizard if installing WinPcap.

🕼 Wireshark 1.8.3 (64-bit) Setup	
Install WinPcap? WinPcap is required to capture live network data. Should WinPcap be insta	alled?
Currently installed WinPcap version WinPcap 4.1.2	
Install Install WinPcap 4.1.2 If selected, the currently installed WinPcap 4.1.2 will be uninstalled	first.
What is WinPcap?	
Nullsoft Install System v2.46	Cancel

j. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.

🍊 Wireshark 1.8.3 (64-bit) Setup		23
Installation Complete Setup was completed successfully.		7
Completed		
Extract: mergecap.html Output folder: C:\Program Files\Wireshark Extract: capinfos.exe Extract: capinfos.html Output folder: C:\Program Files\Wireshark Extract: rawshark.exe Extract: rawshark.html Output folder: C:\Program Files\Wireshark Extract: user-guide.chm Completed		•
Nullsoft Install System v2,46	< Back Next > Can	cel

k. Click **Finish** to complete the Wireshark install process.



# Part 2: Capture and Analyze Local ICMP Data in Wireshark

In Part 2 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

#### Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

- a. Open a command window, type **ipconfig /all**, and then press Enter.
- b. Note your PC interface's IP address and MAC (physical) address.

C:\Windows\system32\cmd.exe	
C:\>ipconfig /all	A
Windows IP Configuration	
Host Name : PC-A Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled : No	
WINS Proxy Enabled No Ethernet adapter Local Area Connection:	
Connection-specific DNS Suffix .: Description	onnection
Autoconfiguration Enabled : Yes Link-local IPv6 Address : f <del>68824ba:a</del> 0a0:9f0:ff88%11(Pre IPv4 Address	eferred)
Default Gateway	0 0D F4 44

c. Ask a team member for their PC's IP address and provide your PC's IP address to them. Do not provide them with your MAC address at this time.

#### Step 2: Start Wireshark and begin capturing data.

a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

b. After Wireshark starts, click Interface List.

WIRESHARK White 242 DWH INVAS	Si him /hink-1.8	
Capture	File	Online
Interface List The sub-transmission Start  Start  Sub-transmission Start  Sub-transmission Sub-transmission Sub-transmission Sub-transmission Sub-transmission Sub-transmission Sub-transmission Capiture Help  Move to Capiture  Rese, seeking and sub-transmission  Capiture Help  Full  Move to Capiture  The sub-transmission  Capiture Help  The sub-transmission  The sub-transmission  The sub-transmission  The sub-transmission  The sub-transmission  The su		Website         Into the population contract         Into Contract Contract         Into Contract Contract         Security         Notified the Website in an executive in population

Note: Clicking the first interface icon in the row of icons also opens the Interface List.

c. On the Wireshark: Capture Interfaces window, click the check box next to the interface connected to your LAN.

Wireshark: Capture Interfaces					- • <b>×</b>
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
Help		<u>S</u> tart	Stop	<u>O</u> ptions	<u>C</u> lose

**Note**: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.

	Wireshark: Interface Details	- • •
[	Characteristics Statistics 802.3 (Ethernet) 802.11 (WLAN) Task Offle	oad
	Permanent station address 00:50:56:BE:76:8	
	Current station address 00:50:56:BE:76:8	C
	Statistics	

d. After you have checked the correct interface, click **Start** to start the data capture.

Wireshark: Capture Interfaces					- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose
		$\sim$			

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

argentical Januaria argentical Januaria (argentical Januaria (a	Terretary 104 Frances 1 Terretary Contraction Spanning-trans- (for- 173, 194, 79, 123 Spanning-trans- (for- 173, 194, 79, 123 Spanning-trans- (for- 173, 194, 127 Spanning-trans- (for- 174, 194, 194, 194 Spanning-trans- (for- 174, 194, 194 Spanning-trans- (for- 174, 194, 194 Spanning-trans- (for- 174, 19	Pysoul L Pysoul L TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	C. D. R. M. S. M. S.           expl. Me.           40 Corff. Nont. + 1778.0.30:47.04:14:04:14           Corff. Nont. + 1778.0.30:47.04:14:04:04           Corff. Nont. + 1778.0.30:47.04:14:04           Corff. Nont. + 1778.0.30:07.07.04:14:04           Corff. Nont. + 1778.0.30:07.07.04:14:04           Corff. Nont. + 1778.0.30:07.01:14:04           Corff. Nont. + 1778.0.30:01:07.01:14:01           Corff. Nont. + 1778.0.30:01:07.01:14:01           Corff. Nont. + 1778.0.30:01:01:14:04           Corff. Nont. + 1778.0.30:01:01:14:01           Corff. Nont. + 1778.0.10:01:01:14:01           Corff. Nont. + 1778.0.10:01:15:01:14:01           Corff. Nont. + 1778.0.10:01:15:01:14:01           Corff. Nont. + 1778.0.10:01:15:01:14:01           Corff. Nont. + 1778.0.10:01:15:01:14:01	
arte 1 26. 10 25. 10 10 25. 75 25. 10 10 25. 75 25. 10 10 25. 10 4. 21 10 25. 10 25. 10 10 25. 10 25. 10 10 25. 10 25. 10 10 25. 10	Det seton Suanting - erran- (for- 173.384,79,325 50,20,344,23 Spanning - erran- (for- 173.36,22,72 10,20,344,23 Spanning - erran- (for- 123.36,27,25 Spanning - trans- (for- 123.36,27,25)	C C C C C C C C C C C C C C C C C C C	Comparison         Comparison <thcomparison< th="">         Comparison         Comparis</thcomparison<>	
1000 1000	Dectantion Example and the second se	Pressual L Pressual L TCP TCP TCP TCP TCP TCP TCP TCP TCP	NVM         State         S	
1200 70.000 70 1200 70.000 10 1200 70 100 10 100 10 10 100 100 10 100 100 10 100	Det action	Pressual L TCP TCP TCP TCP TCP TCP TCP TCP TCP TCP	Apr.         Apr.           40 Currf Boost = 11718.0130/rff 0rf1sor:34 Curst = 0 Pert = ItaB001           91 Trts Segment of a readsampling poul           90 wepp client + 53388 [acc] sequitacts # 0.002 Len-0           90 wepp client + 53388 [acc] sequitacts # 0.002 Len-0           90 currf Boost = 27100 (710/rff 0rff) sequitacts # 0.002 Len-0           90 currf Boost = 27100 (710/rff) off sequitacts # 0.002 Len-0           90 currf Boost = 27100 (710/rff) off sequitacts = 0 Pert = 0.0001           90 currf Boost = 27100 (710/rff) off sequitacts = 0 Pert = 0.0001           91 Signed & 19848 [acc] sequitacts = 0 Pert = 0.0001           92 Signed & 19848 [acc] sequitacts = 0 Pert = 0.0001           92 Signed & 19848 [acc] sequitacts = 0 Pert = 0.0001           94 Obtion = 5.37660 [acc] sequitacts = 0 Pert = 0.0001	
1,20,164,21 1,21,164,21 1,21,164,21 1,21,164,21 1,25,164,21 1,25,164,21 1,25,164,21 1,3,36,12,73 1,20,164,21 1,65,57,53 1,20,164,21 1,66,21 1,65,21 1,66,57,53 1,66,21 1	Sparrer 19, 2019 Sparrer 19, 2019 19, 2019 19, 201, 204, 23 Sparrer 19, 27, 204 Sparrer 19, 27, 204 19, 201, 204, 23 Sparrer 19, 27, 204 19, 201, 204, 204 Sparrer 19, 27, 27, 27, 27, 27, 27, 27, 27, 27, 27	100 100 100 100 100 100 100 100 100	40 Corff. Bost: = 11718.0.030:F7.0f.14.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.24.0f.26.0f.25.0f.26.0f.	
N20, 194, 19 31, 194, 79, 125 1960, 74, 196, 195 1960, 74, 196, 194 1960, 74, 196, 24 1960, 74, 197, 24 197, 34, 137, 73 197, 74, 167, 194 2, 20, 196, 21 1, 66, 57, 53 2, 20, 196, 21	273.194, 75, 223 173.194, 75, 223 10, 20, 564, 23 Gaarning, trans. (For- lipareting, trans. (For- 173.36, 12, 72 10, 20, 184, 23 Enzyment, trans. (For- 174.65, 37, 33	10P 10P 11P 10P 10P 10P	01 TTCP segment of a featsenflet POU] 60 wapp client 53586 [acc] seq.4 acSa 8 win=1002 [eo-d 60 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 60 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 60 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 60 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 60 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 61 conf. wort = 27740 (r.30+7.05 feat.24 cont = 0 wort = 0.00051 53 33966 + 19846 [acc] seq.4 acSa win=331 acm=0 Mini 984=2 64 10446 - 37466 [acc] seq.4 acSa win=34 kinet 0 Mini 984=2	
A. 20, 105, 21 31, 194, 79, 125 1950, 71, 195, 36 1950, 71, 195, 36 1950, 71, 195, 36 1950, 71, 195, 37 1950, 71, 195, 21 13, 36, 12, 72 14, 65, 57, 53 1, 56, 57, 53 1, 50, 57, 55 1, 50, 57, 55 1, 50, 57, 57 1, 50, 57,	10, 20, 204, 21 50, 20, 244, 21 Spanning-trive-(for- liparning-trive-(for- 173, 36, 12, 72 10, 30, 184, 23 Spanning-trive-(for- 271, 68, 57, 53		11 (111) Segment of a real-seminer your 10 segment of a real-seminer your 10 segment of a real-seminer your 10 conf, sout = 2710.0 (10 177-06; 4) actisk (101 ± 0) fort = 0.0001 10 conf, sout = 2710.0 (10 177-06; 4) actisk (101 ± 0) fort = 0.0001 10 conf, sout = 2710.0 (10 177.06; 7) actisk (101 ± 0) fort = 0.0001 15 53964 + 10846 [acx] sequel actisk wines3914 (1001 ± 0) 40 (10446 > 33966 [acx] sequel actisk wines3914 (1000 5,841 966-2)	
31234, 791223 920, 741, 921, 54 920, 741, 921, 54 920, 741, 921, 54 920, 741, 921, 54 920, 741, 921, 54 93, 24, 13, 73 1077, 74, 95 1, 65, 57, 53 1, 66, 57, 53 1, 66, 57, 53 1, 66, 57, 53 1, 66, 57, 53 1, 50, 164, 21	201 201 204 204 Spanning-tries-(for- liparning-tries-(for- dparning-tries-(for- 173, 36, 127 as- 10, 20, 344, 73 Spanning-tries-(for- 171, 66, 37, 33	107 87 1079 17 1079 17 1079 17 1079 17 1079 17 1079	00         00000         0000         0000	
940, 79, 94, 18 940, 79, et 18 7, 36, 12, 72 97, 36, 12, 72 97, 73, 85, 18 1, 66, 57, 53 1, 66, 57, 53 1, 66, 57, 53	Lparming-true-(for- dparming-true-(for- 173, 36, 12, 72 10, 20, 344, 23 Sparming-true-(for- 171, 66, 37, 33	1070 1070 1070 1070 1070	60 Conff, Root = X1790 (0.30; 77:06; 74:04; 44 Cont = 0 Furt = 0.8051 60 Conff, Root = X1790 (0.30; 77:06; 74:04; 44 Cont = 0 Furt = 0.8051 55 S1964 = 136846 [ArX] Seq4: ArX=0 win=511 } Lond 64 10846 > 53966 [ArX] Seq4: ArX=0 win=511 Lond 54.10846 > 53966 [ArX] Seq4: ArX=0 win=511 Lond	
510, 74, 61, 75 3, 30, 164, 21 3, 36, 13, 73 5, 20, 164, 21 1, 68, 57, 53 5, 20, 164, 21	Spanne (rg Crass., Crass.) 173, 36, 12, 72 10, 20, 344, 23 Spanne (rg Crass., Crass.) 171, 66, 37, 53	109 109 109	64 10446 A 10466 Sax3 See3 Adva Mines301 (064 - 0 mine a minor) 57 53966 A 10466 Sax3 See3 Adva Mines301 (064 - 0 mine a minor) 60 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a minor) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a minor) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) 61 contr, more - streng Oxio (064 - adva mines1) (164 - 0 mine a mines1) (164 - 0 mine a mines1) (164 - 0 mines1)	
20, 164, 21 3, 36, 13, 73 5, 20, 164, 21 1, 68, 57, 53 5, 20, 164, 21	173, 36, 12, 72 10, 20, 144, 21 10171, 65, 37, 53	TCP TCP TCP	55 53964 + 19846 [ack] seq=1 ack=1 win=63974 [et=1 66 10846 + 53966 [ack] seq=1 ack=2 win=513 [att=0 \$6,6=1 \$86=2	
3, 36, 13, 73 	10, 20, 344, 23 Sparstra-traes(1st-) 271, 68, 57, 53	TEP	60 10846 > 53966 [aCK] Seq=1 Ack=2 wire-513 Len=0 56,6=1 086=2	
1.00.104.21 1.68.57.53 2.20.164.21	Spanning-12 ee (1 cm-) 271.08.37.53	e ste	An index a light Peril Solar work structs three whet is a	
20,164,21 1,68,57,53 2,20,164,21	171.08.57.53		and a server as a server of the server of the server as the server of th	
1.68.57.53	40 10 40 40 A	Land Land	67 king course but intro 2, 10.	
20.164.21		ALC: NOT THE OWNER OF	We want good you wanted a semilart and page door how avera	
	173 27 115 100	NEW	50 Name (prov) ( Springer, Registration many and the strate	
3, 57 315 1.01	10.20.164.25	ALC: NO.	10 Name might cannot a langestad mate does not exist	
30.164-21	10.20.364.33	Autoric .	17 kass mere in intra-2-30-	
20, 162, 21	10.20.164.35	NUMBER	50 NAME DATY IS UNIT 2.10	
and Carpen al	Enginetation of the literal	- 67P	10 iner, herr - 12265 0 10 PT OF TAIRCHE LART - 0 FIFT - 0a1001	
20 164 21	10.30 144 15	NUMBER	02 Manu many Mill (MT0/1/20)	
20.164.21	121.68.52.51	MARKS .	62 Mane Houry MR (MTTX \$220)	
1.68.57.33	10.20.164.21	NEMS	50 have mery records, temested name doet not evict	
20, 164, 21	171.77.115.191	NUM	62 Name marry MR UNITY 3-205	
3, 17, 115, 300	10,20,164,21	MEMS	55 Name many response. Requested many down not exist	
20.164.21	10.20.164.11	10015	92 Name Direct MR UNITE \$420+	
20.164.21	30, 20, 164, 31	NUM	92 Name Datery MR UNDO 3-20-	
NED TACKSTEE	Spaceton-trea-Mor-	IT STE	40 cost, most - 12764 0 10 17 0d: anarila Cust - 0 surt - 048001	
20,164,21	107.108.87.9	SRVLOC	50 Attribute Request, VI Transaction 20 - 40259	
A CONTRACTOR OF				
	.20.164.21 20.164.21 1.68.37,53 20.164.21 1.68.37,53 20.164.21 20.	120.164.21         10.70.164.13           20.164.21         17.065.57.53           1.66.57.53         10.20.164.22           20.164.21         17.167.164.23           3.57.153.101         10.70.164.23           20.164.21         10.70.164.23           20.164.21         10.70.164.33           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.34           20.164.21         10.70.164.30           20.164.21         10.70.164.30           20.164.21         10.70.164.30	120.164.21         10.20.164.11         WHK           120.164.21         171.64.57.55         WHK           1.66.57.51         10.20.164.22         WHK           1.66.57.51         10.20.164.22         WHK           1.66.57.51         10.20.164.21         WHK           1.70.164.21         10.20.164.31         WHK           2.01.164.21         10.21.164.21         WHK           2.01.164.21         10.21.164.21         10.20.164.21           2.01.164.21         10.21.164.21.01.00.164.21.01.01         11.24.20.10.01           2.01.064.51         10.21.10.20.164.21.01.01.01         10.21.10.01	120.164.21         10.20.164.11         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         17.165.57.35         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         17.165.171         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         17.17.155.171         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         10.20.164.12         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         10.20.164.12         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         10.20.164.13         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         10.20.164.13         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         10.20.164.13         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         20.20.164.13         MMMS         00 Harm query ML MUDIC-COD- 20.166.21         20.20.164.21         20.20.164.21         20.20.164.21         20.20.20         20.20.20           20.166.21         10.20.164.25.21         10.20.164.25         10.20.164.25         10.20.164.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26         20.20.26

e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the Filter box at the top of Wireshark and press Enter or click on the **Apply** button to view only ICMP (ping) PDUs.



f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and **ping the IP address** that you received from your team member. Notice that you start seeing data appear in the top window of Wireshark again.

ile Edit View Gn	Canture Analyze Stati	dirs Telephony Tonis I	csvnu Rev 38096	strom /trunk-1.0	01		19.13	부대 역
	BOXCA	0.00073		aaa	c 🖉 🕅 🗧	3 × B		
ilter icmp		1	· Expression	Clear Apply				
o. Time	Source	Destination	Protocol L	ength Info				
11 15.118840	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) reques	t id=0x0001.	seq=21/5376,	tt]-1
14 15.119602	192.168.1.12	192.168.1.11	IONS	74 Echo	(ping) reply	1d=0x0001.	seq=21/5376,	111=1
16 16.127853	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) reques	t 1d=0x0001,	seq=22/5632,	tt]=1
17 16.128679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	1d=0x0001.	seq=22/5632,	ttl-1
18 17.141897	192.168,1.11	192.168.1.12	ICMP	74 Echo	(ping) reques	t 1d=0x0001.	seq=23/5888,	1=121
19 17.145943	192.168.1.12	192.168,1.11	ICMP	74 Echo	(ping) reply	1d=0x0001,	seq=23/5888,	ttl=1
21 18.140246	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) reques	t 10=0x0001,	seq=24/6144,	tti-1
SE TO- 1401 34	A76+ 200+ 2 - 22	196+190+1+A1	10.00	LA ECHO	(build) rebits	10000001	Selfaral Araa	
Frame 11: 74 b Ethernet 11, S Internet Proto Internet Contr	ytes on wire (592 rc: Vmware_be:76:8 col version 4, Src ol Message Protoco	Tunnel adapter Hedia State Connection Physical Add Control (1997) Physical Add MicP Enabled Autoconfigur Ci>> Ci>>ping 192.16	Local Area pecific DN pers ation Enab	Connection È Suffix	* 11: : Media dis: : Terede Tu: : D0-00-00-1 : No : Yes	connected weling Pseud 30-00-00-5	o-Interface 8	
	a F6 db 00 50 56 /	Pinging 192.168 Reply from 192. Maply from 192.	1.1.12 with 168.1.12: 168.1.12:	32 hytes o hytes-32 ti hytes-32 ti	f data: ne-ins IIL-1: ne(ins IIL-1:	28		

**Note**: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Please see

Appendix A: Allowing ICMP Traffic Through a Firewall for information on how to allow ICMP traffic through the firewall using Windows 7.

g. Stop capturing data by clicking the **Stop Capture** icon.



#### Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member's PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers, and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

Cap	turin 5 da	g fro	m Int	el(IR) P	RO/	1000 7	MTNe	two	rk Co	necti	ion	[Wir	esha	nk1	61 (	SVN Rev 3809	5 fror	n /trunk-1.	6)]						0	0	x
Ene s	t a	Tier	v g V m		iptur		nayze	2		6 I	eiep	nony ab	4	500	-pro 	ernais deip	0	0.0	en.	-	1 671 <b>#1</b>	30 18					
	1		-				14 14	1.12	=		<i>a</i> .	-	-		-	(moles)			( hand ( )	-	- 1607 - <b>16</b> 0	100					
Filter	icm	P													10	Expression	Cle	ter Apply									
No.	T	ime		S	ource	e	100	6		Des	timat	ion	-			Protocol I	engt	h Info		-		10.00			1000		-
	11 1	5.1	188	0 1	92.	165.	1, 1			19	2.1	68,1	1.1	2		ICMP		74 Echo	Cpin	9)	request	1d-0x0	1001	seq-2	1.5376	, tt	1-1.
2	14 1	5.1	1960	12 1	92.	168.	1.1.	2		19	2.1	68.1	1,1	1		ICMP	- 3	74 Echo	(pin	g)	reply	id=0x0	001	seq=2	1/5376	, tt	l=li
-	16 1	.6.1	278	3 1	9Z.	168.	1.11	-		19	2.1	68.1		2		ICMP	-	74 Echo	(p1n	g)	request	1d=0x0	001	seq=2	2/5632	, tt	1=1;
	1/ 1	0.1	280	9 1	92.	168.	1.1.	<u>.</u>		19.	. 1	08.1		1		ICMP	_	4 ECho	(pin	a)	repty	1d=0xt	1000	seq=2	2/3032		1-1.
	10 1	2.1	410		36.	100.	4 47	-		19		00.1		-		TCMP	- 3	4 ECHO	(pin	묏.	request	Id=0x0	NOU1	seq=2	3/3008		1-11
1	27.1	9.4	4094	5 1	92.	168	1 11	С. 1.		10	6 - A 3 - T	00.J				TCMP		74 Echo	(pin	97	repry	id-0xt	1001	sed-t	3/ 300a		7-1-
	22 1	8 1	4079	M T	07	168	1 1			10	2 1	68.1		1		TCMP		74 Echo	(nin	22 20	request	ideox	001	seg=2	4/6144	+++	1-1:
0 Fra 0 Eth 0 Int 0 Int	ame hern tern	11: Net	74 II, Prot	byte src oco rol	es o Ir Mes	on w ntel ersi isag	ire Cor_ on 4 e Pr	(59 34: , 5 oto	2 bi 92:1 rc: col	its) c ( 192	, 7 58: .16	4 by 94:0 8.1.	yte 5b: .11	s c 34: (1	apti 92:1 92.1	ured (592 Lc), Ost: L68.1.11)	bit Int Ds	s) el_Of:9 it: 192.	91:48 168.1	(0 L.1	0:11:11 2 (192.)	:0f:91:4 L68.1.12	8) )				
0000 0010 0020	00 00 01	50 3c 0c	56 01 08	be f ac 0	6 d 0 0 d 4	b 00 0 80 6 00	0 50 0 01 0 01	56 b3	5 be 5 ad	76 c0 61	5c a8 62	08 01 63	00 0b 64	45 c0 65	00 a8 66	. PV .<	P V	.vE.					Bo	ddle Sec ttom Sec	tion		
0030 0040	67 77	68 61 PRO/	69 62	63 6 03 6	6 6 4 6	ic 60 5 60 rk Cdi	d 6e 5 67 nnecti	61 61	F 70 8 69	71 ickets	72	7.3 Disp	74 laye	75 d:8	76 Marki	ghijkle wabcdef ed:0	n o g h	pqrstuv 1				Prof	le: Del	ault			•

a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC's IP address, and the Destination contains the IP address of the teammate's PC you pinged.

Intelis	R) PRO/1000 MT	Network Connection [N	Nireshark 1.6.1 (SVN Rev 3805	6 from /trunk-1.6)]					-ca-1-0	
Eile Ed	it <u>Y</u> iew <u>Go</u>	Capture Analyze Sta	itistics Telephony Tools	Internals Help						Kours
製板		😑 🖬 🗶 🖉 🖉	C + + + = 7	1	2 Q Q	1	1 🖾 🥵	\$\$ I 🖬		pouro
Filter:	cmp			Expression	Clear Apply					
No.	Time	Source	Destination	Protocol Ler	igth Info					
5	2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=25/6400.	ttl=1;
1	8 2.802679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001.	seq=25/6400,	ttl-17
10	3.816895	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id-0x0001.	seq-26/6656,	tt]-11
11	3.817540	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id~0x0001.	seq-26/6656.	tt1-1:
1 5	4.831548	192.168.1.11	192 168 1.12	ICMP	74 Echo	(01001	request	d-0x0001.	seg=27/6912.	REIDE
-14	4.832006	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	repty	id=0x0001,	seq=27/6912,	ttlali
15	5.844858	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001.	seq=28/7168,	ttl=1:
16	5 5.845488	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001.	seq=28/7168,	tt]=1;

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the Destination and Source MAC addresses.

Iter: icmp			Expression.	Clear	Apply					
. Time	Source	Destination	Protocol	Length	Info					
5 2.801784	192.168.1.11	192.168.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq=25/6400.	tt]=]
8 2.802679	192,168,1,12	192.168.1.11	ICMP	74	Echo	(ping)	reply	1d=0x0001.	seq=25/6400.	ttl=1
10 3.816895	192.168.1.11	192.168.1.12	ICMP	74	Echo	(ping)	request	1d=0x0001.	seq=26/6656	ttl=
11 3.817540	192.168.1.12	192.168.1.11	ICMP	74	Echo	(ping)	reply	Id=0x0001,	seq=26/6656.	ttl-
13 4.831343	192.168.1.11	192.168.1.12	ICMP	74	Echo	(ping)	request	id=0x0001,	seq-27/6912.	ttl-
14 4.832006	192.168.1.12	192.168.1.11	ICMP	74	Echo	(ping)	reply	id=0x0001,	seq=27/6912,	ttl-
15 5.844858	192,168,1,11	192,168,1,12	ICMP	74	Echo	(ping)	request	1d=0x0001,	seq=28/7168.	ttl=
16 5,845488	192,168,1,12	192,168,1,11	ICMP	74	Echo	(p1ng)	reply	1d=0x0001,	seq=28/7168	tt]=]
Frans 13: 74 b Ethernet II, S Destination: Bource: Inte	rc: IntelCor_34:92 Intel_Of:91:45 (0 Cor_34:92:10 (58	bits), 74 bytes cap 21c (36:91:6b:34:92 00:11:11:0f:91:48) 94:6b:34:92:1c)	tured (392 :1c), Dst:	bits Inte	) 1_0f:9	1:48 ((	90;11;11	:Of:91:48)	_	_

Does the Source MAC address match your PC's interface?

Does the Destination MAC address in Wireshark match the MAC address that of your team member's?

How is the MAC address of the pinged PC obtained by your PC?

**Note**: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

# Part 3: Capture and Analyze Remote ICMP Data in Wireshark

In Part 3, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 2.

#### Step 1: Start capturing data on interface.

a. Click the Interface List icon to bring up the list PC interfaces again.



b. Make sure the check box next to the LAN interface is checked, and then click Start.

📶 Wireshark: Capt	ure Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

c. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



d. With the capture active, ping the following three website URLs and answer questions on sheet.

www.yahoo.com www.cisco.com www.google.com

```
C:\Vindows\system32\cmd.exe
C:\>ping www.yahoo.com
Pinging www.shoo.com
Pinging www.shoo.com
Pinging www.cisco.com
Pinging www.google.com
Pinging www.google.com
Pinging www.google.com
Pinging www.google.com
Pinging www.google.com
Pinging www.google.com
Ping statistics for 794.125.129.991 with 32 bytes of data:
Reply from 74.125.129.99: bytes=32 time(Ims TIL=255
Reply from 74.125.129.99: bytes=32 time(Ims
```

**Note**: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

e. You can stop capturing data by clicking the **Stop Capture** icon.



## Part 4: FTP PDU Capture

Step 1: Start packet capture.

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the Start option on the Capture menu of Wireshark.

At the command line on your computer running Wireshark, enter ftp ftp.heanet.ie

When the connection is established, enter anonymous as the user without a password.

Userid: anonymous

Password: <ENTER>



Type bye to close the ftp session and stop the packet capture in Wireshark.

Examine Packet Details.

Select (highlight) a packet on the list associated with the first phase of the FTP process.

View the packet details in the Details pane.

What are the protocols encapsulated in the frame?

Highlight the packets containing the user name and password.

Examine the highlighted portion in the Packet Byte pane.

What does this say about the security of this FTP login process?

## Part 4: HTTP PDU Capture

Step 1: Start packet capture.

Assuming Wireshark is still running from the previous steps, start packet capture by clicking on the Start option on the Capture menu of Wireshark.

Note: Capture Options do not have to be set if continuing from previous steps of this lab.

Launch a web browser on the computer that is running Wireshark.

Enter the URL of a website eg. <u>www.rte.ie</u> . When the webpage has fully downloaded, stop the Wireshark packet capture.

Step 2: Increase the size of the Wireshark Packet List pane and scroll through the PDUs listed.

Locate and identify the TCP and HTTP packets associated with the webpage download.

Note the similarity between this message exchange and the FTP exchange.

Step 3: In the Packet List pane, highlight an HTTP packet that has the notation "(text/html)" in the Info column.

In the Packet Detail pane click on the "+" next to "Line-based text data: html"

When this information expands what is displayed?

Examine the highlighted portion of the Byte Panel.

This shows the HTML data carried by the packet.

#### Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

## Appendix A: Allowing ICMP Traffic Through a Firewall

If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

#### Step 1: Create a new inbound rule allowing ICMP traffic through the firewall.

a. From the Control Panel, click the **System and Security** option.



From the System and Security window, click Windows Firewall.



b. In the left pane of the Windows Firewall window, click Advanced settings.



c. On the Advanced Security window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.

Attion	
Inbound Rules	
<ul> <li>New Rule</li> <li>♥ Filter by Profile</li> <li>♥ Filter by State</li> <li>♥ Filter by Group</li> <li>View</li> <li>Refresh</li> <li>Export List</li> </ul>	• • • •
	View CRefresh Export List Help

d. This launches the New Inbound Rule wizard. On the Rule Type screen, click the **Custom** radio button and click **Next** 



e. In the left pane, click the **Protocol and Ports** option and using the Protocol type drop-down menu, select **ICMPv4**, and then click **Next**.

Protocol and Ports		
Specify the protocols and ports to	a which this rule applies.	
Steps		
· Rule Type	To which ports and protocols does this rule apply?	
Program     Detect		
Protocol and Ports	Protocol type: Any 🔹	
a pcope	Protocol number: Any Custom	
<ul> <li>Action</li> </ul>	- AND	
<ul> <li>Profile</li> </ul>	Local port: GMP	
<ul> <li>Name</li> </ul>	TCP UDP	
	Pv6 Pv6-Bote	
	Perrote port: IPv6-Frag	
	ICMPv6	
	IPv6NoNd IPv6Ovv	
	Internet Control Message VRRP	
	(ICMP) settings PGM L2TP	
	The second second second second second	
	Learning a good proceed and porta-	
	< Back	Next > Cancel

f. In the left pane, click the Name option and in the Name field, type Allow ICMP Requests. Click Finish.

🔗 New Inbound Rule Wizard		×
Name		
Specify the name and description	n of this rule.	
Steps:		
Rule Type		
Program		
Protocol and Ports		
Scope	Name.	
Action	Allow ICMP Requests	
Profile	Description (optional):	
Name		
$\smile$		
	$\frown$	
	Karter Sack (Finish) Cancel	

This new rule should allow your team members to receive ping replies from your PC.

#### Step 2: Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of Inbound Rules.

a. On the Advanced Security window, in the left pane, click **Inbound Rules** and then locate the rule you created in Step 1.

Windows Firewall with Advances	d Security					0	2
File Action View Help							
Windows Formal with Advance	Inbound Rules					Actions	
Contraction Rules	Near Allow KMP Requests O Tarve TAU 2 Distington Standard Entron bin © Jave(TM) 2 Platform Standard Edition bin © Jave(TM) Platform St binary © Jave(TM) Platform St binary © winzdius exe © minzdius exe © minzdius exe	Group BranchCache - Content Retr	Private Private Private Private Private Private Private Private Private All	Enabled Ves Yes Yes Yes Yes Yes Yes No	Action Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	Indexund Rules     New Rute     V Filter by Profile     V Filter by State     V Filter by Group     View     Refresh     Export List     Help	
	BranchCache Hinsted Cache Server (HTT BranchCache Peer Discovery (WSD-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (TCP-In) Connect to a Network Projector (WSD Ev Connect to a Network Projector (WSD Ev	BranchCache - Hosted Cach BranchCache - Peer Discove Connect to a Network Proje Connect to a Network Proje	All All Domain Private Private Domain Domain Private	No No No No No No	Allow Allow Allow Allow Allow Allow Allow	Allow ICMP Requests  Chable Rule  Cut  Cut  Copy  Cut  Seleta  Deleta  Copy	•

b. To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between Disable Rule and Enable Rule; the status of the rule also shows in the Enabled column of the Inbound Rules list.

Fée Action View Help									
P Windows Firewall with Advance	Inbound Rules						Actions		
Inbound Rules	Name	Group	Profile	Enabled	Action		Inbound Rules		
Connection Security Bules	Colore 20MD Requests		All C	Yes	Allow		New Rule		
Monitoring	2 Java(TM) 2 Platform Standard Edition bin	4	Private.	Yes	Allow		T Filter by Perdile		
1 Mail 1000	2 Jave(TM) 2 Platform Standard Edition bin		Private	Ves	Allow		The systems		
	W Java(TM) Platform SE binary		Private	Ves	Allow	1.3	W Fifter by State	1	
	2 Java(TM) Platform SE binary		Private.	Yes	Allow		Tilter by Group		
	@ winradius.exe		Private:	Ves	Allow		View		
	🕲 winradius.au		Private	Ves	Allow		Refuel		
	🕲 winradius.exe		Private.	Yes	Allow		E vauen		
	O winradius.exe		Private.	Ves	Allow		Export List		
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	Nei	Allow		Help		
	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	Allow		And the second se		
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	AH	No	Allow	12	Allow IC MP Requests		
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain	No	Allow	<	Disable Rule		
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private	No	Allow		1 Cut		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje-	Private	No	Allow		R. Court		
	O Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		dill copy		
	Connect to a Network Projector (WSD Ev	Connect to a Network Projs	Domain	No	Allow		× Delete		

c. To permanently delete the ICMP rule, click **Delete**. If you choose this option, you must re-create the rule again to allow ICMP replies.

it iveti	All	INU	Allow		1	пер
I Cach	All	No	Allow			
iscove	All	No	Allow		Allo	w ICMP Requests
Proje	Domain	No	Allow		۲	Disable Rule
Proje	Private	No	Allow		X	Cut
Proje	Private	No	Allow		en.	Comu
Proje	Domain	No	Allow		비비	Сору
Proje	Domain	No	Allow	$\square$	×	Delete
Proie	Private	No	Allow		F	Properties