

## CS450 – Introduction to Networking Lecture 15 – Wireshark & Assignment 3

Phu Phung Feb 16, 2015

# Information

• Website:

https://www.wireshark.org/

• Labs from Textbook

http://www-net.cs.umass.edu/wireshark-labs/

# What is Wireshark?

- Wireshark is a network packet/protocol analyzer.
  - A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- "The World's Most Popular Network Protocol Analyzer"

# Wireshark System Overview



# Install under Windows

Z T

- Download
- Install

	This wizard will guide you through the installation of Wireshark. Before starting the installation, make sure Wireshark is not	
<b>Vireshark 1.0.0 Setup</b> Installing Please wait while Wireshark 1.0.0 is being installed.	Click 'Next' to continue.	
Extract: faq.txt Output folder: C:\Program Files\Wireshark\wimaxasncp Extract: dictionary.xml Extract: dictionary.dtd Output folder: C:\Program Files\Wireshark Output folder: C:\Program Files\Wireshark\help Extract: toc Extract: overview.txt Extract: getting_started.txt Extract: capturing.txt Extract: capturing.filters.txt Extract: display_filters.txt Extract: faq.txt	Image: State of the state	
Julisoft Install System v2.33	This product is brought to you by	
	Nullsoft Install System v2.16	

✓ Vireshark 1.0.0 Setup

- 🗆 X

Welcome to the Wireshark 1.0.0

Setup Wizard

## Install under Debian/ Ubuntu

#### • # apt-get install wireshark

The Wireshark Network Analyzer								
<u>File Edit View Go Capture Analyze Statistics H</u> elp								
	🗐 🕞 🔍 🍳 🔍 🔛 📓 🕺 🖉							
<u>F</u> ilter:	Expression Clear Apply							
	Winscharle Cantum Interferen		-			0	X	
	wireshark: Capture Interfaces							
	Description	IP	Packets	Packets/s		Stop		Â
	. Broadcom 440x 10/100 Integrated Co	ontroller 192.168.0.100	0	0	Start	Options Det	ails	
	🛒. Microsoft	192.168.0.28	276	25	Start	Options Det	ails	
	🛒. MS Tunnel Interface Driver	unknown	0	0	Start	Options Det	ails	111
Ready to load or capture No Packets	🛒. VMware Virtual Ethernet Adapter	192.168. <mark>28.</mark> 1	0	0	Start	Options Det	ails	
	🛒. VMware Virtual Ethernet Adapter	192.168.48.1	0	0	Start	Options Det	ails	
	Help					Close		-
								-

# Configuration

This checkbox allows you to specify that Wireshark should put the interface in **promiscuous** mode when capturing. If you do not specify this, Wireshark will only capture the packets going to or from your computer (not all packets on your LAN segment).

🔀 Vireshark: Capture Options	_ 🗆 ×
Capture	
Interface: Intel (R) PRO/Wireless 3945ABG Network Conne	ction (Microsoft's Packet Scheduler) 💌
IP address: 192.168.18.202	
Link-layer header type: Ethernet 🕶 Buffer size: 1	🔹 megabyte(s) Wireless Settings
Capture packets in promiscuous mode	
Limit each packet to 68	
Capture Filter:	
,	
Capture File(s)	Display Uptions
File: <u>B</u> rowse	🔽 <u>U</u> pdate list of packets in real time
Use multiple files	
Next file every 1 megabyte(s) 🗸	▶ Automatic scrolling in live capture
Next file every 1 minute(s) 🔻	🗹 Hide capture info dialog
✓ Ring buffer with 2 files	Name Resolution
☐ Stop capture after 1 ★ file(s)	
Stop Capture	J♥ LNADIE MAC Name resolution
1 * packet (s)	Enable <u>n</u> etwork name resolution
megabyte(s)	
□ after 1 ★ minute(s) ▼	✓ Enable <u>t</u> ransport name resolution
Help	<u>S</u> tart <u>C</u> ancel

# Wireshark Interface



# Wireshark on VirtualBox

- Only work with Ethernet interface
  - Bridge Adapter
  - Run with root permission:
    - \$sudo wireshark

### Wireshark on VirtualBox

resha	rk						😻 🖂 📼 ঝ 🕕 12:46 PM 上 phu
Q,	800	phu@phu-\	/irtualBox:				
		Wireshark:	Capture fro	om eth0	tistics Telephony Tools	Internals Help	D
	Captured	Packets			🕴 🖴 🔍 🤶 🔶 🖞	) T 1	🗏 📑 e e 🛛 📅 📓 陸 💥 l
	Total	1755	% of total				
	SCTP	0		0.0%	▼ Expres	sion Clear	Арріу
2	UDP	707		40.3%	Destination	Protocol Leng	gth Info
	ICMP	10		0.6%	131 103 185 255		00 Who has 131.193.185.14/? Tett 131.193.185.1
	ARP	812		46.3%	Broadcast	ARP	60 Who has 131,193,185,17 Tell 131,193,185,108
	GRE	0		0.0%	Broadcast	ARP	60 Who has 131.193.185.32? Tell 131.193.185.1
2%	NetBIOS	0		0.0%	Broadcast	ARP	60 Who has 131.193.185.129? Tell 131.193.185.1
		0		0.0%	Broadcast	ARP	60 Who has 131.193.185.91? Tell 131.193.185.1
	Other	79		4.5%	Broadcast	ARP	60 Who has 131.193.185.228? Tell 131.193.185.1
	I2C Event	s 0		0.0%	Broadcast	ARP	60 Who has 131.193.185.92? Tell 131.193.185.1
	I2C Data	0		0.0%	Broadcast	ARP	60 Who has 131.193.185.68? Tell 131.193.185.1
19	Running	00:02:31			Broadcast	ARP	60 Who has 131,193,185,1552 Tell 131,193,185,1
2	Help			Stop	Broadcast	ARP	60 Who has 131.193.185.2? Tell 131.193.185.1
	( note		l	bcop	::{ff02::1:3	LLMNR	90 Standard query A JMUENCH-PC
	▶ Frame 1:	: 92 bytes	on wire (	736 bits), 9	92 bytes captured (736	oits)	
	Ethernet	t II, Src:	a8:20:66:	3e:54:a1 (a8	8:20:66:3e:54:a1), Dst:	Broadcast (f	f:ff:ff:ff:ff)
9	Internet	t Protocol	Version 4	, Src: 131.	193.185.151 (131.193.18	5.151), Dst: 1	131.193.185.255 (131.193.185.255)
4	0000 ff	ff ff ff f	f ff a8 20	66 3e 54	al 08 00 45 00	. f>TE.	
	0010 00 4	4e bc 1c 0	0 00 40 11	43 69 83	c1 b9 97 83 c1 .N	@. Ci	
	0020 b9	tt 00 89 0 00 00 00 0	0 89 00 3a	8c 8b 4d	44 01 10 00 01	.:MD	
	0030 00 0			72 41 43	+0 50 40 50 45	A DACFFFFE	

### Wireshark on VirtualBox

resha	rk			😻 🖂 📼 👣 🜒 12:47 PM 👤 phu
	80	😣 🗖 🔹 Wireshark: Capture Options		
9	File I	Capture		
		Interface: eth0	~	c) 🗆 🕅 📅 🔛 🔀 🔀
		IP address: 131.193.185.146, fe80::a00:27ff:fecf:4a22	,	
	Filter:	Link-layer header type: Ethernet 💲	Buffer size: 1 ‡ megabyte(s)	
	No.	Capture packets in promiscuous mode		31 193 185 317 1611 131 193 185 1
	18	Capture packets in monitor mode		.31.193.185.94? Tell 131.193.185.1
	18	Capture packets in pcap-ng format		.31.193.185.173? Tell 131.193.185.1
	18	□ Limit each packet to 65535 ‡ bytes		.31.193.185.15? Tell 131.193.185.1
20%	18	Capture Filter:	The second secon	V NB WPAD<00>
	18		Disalar Octions	ort: 44200 Destination port: 32412
	18		Display Options	rt: 54030 Destination port: 32414
1	18	File: Browse	👿 Update list of packets in real time	.31.193.185.254? Tell 131.193.185.1
	18	Use multiple files		31.193.185.176? Tell 131.193.185.1
22	18	Next file every 1 ‡ megabyte(s) ‡	Automatic scrolling in live capture	31.193.185.24? Tell 131.193.185.1
	18	Next file every 1 ‡ minute(s) ‡	Hide capture info dialog	.31.193.185.67? Tell 131.193.185.1
	▶ Fram	Ring buffer with 2 files		
	Ethe ▶ Inte	Stop capture after 1 * file(s)	Name Resolution	t:tt) 255 (131 193 185 255)
9	Tirce		Enable MAC name resolution	
	0000	Stop Capture	_	
	0020	u after	Enable network name resolution	
	0030	🗌 after 1 🌲 megabyte(s) 🛟		

# Display Filters (Post-Filters)

- Display filters (also called post-filters) only filter the view of what you are seeing. All packets in the capture still exist in the trace
- Display filters use their own format and are much more powerful then capture filters

# **Display Filter**

📶 Tucker Ellis & West The Wireshark	: Network Analyzer	
<u>File Edit View Go</u> Capture <u>A</u> naly	ze <u>S</u> tatistics <u>H</u> elp	
	※ 22 ≜   0, 0 ⇒ ∞ 7 ½   目 🖬   0, 0, 0	2. 🖾   🕰 🗹 🛛 🗸
Filter: ip.addr == 192.168.0.1	L Expression ⊆lear Apply	
8/11 Channel: 🔹 🗸	hannel Offset: FCS Filter: Decryption Mode: Non	ie 🗸
Wiresha	ark: Display Filter	
Edit	Filter	
1	Ethemet address 00:08:15:00:08:15	
	Ethemet type 0x0806 (ARP)	
New	Ethemet broadcast	
	No ARP	
	IP only	
	IP address 192.168.0.1	
	IP address isn't 192.168.0.1, don't use != for this!	
	IPX only	
Delete	TCP only	
	UDP only	
	UDP port isn't 53 (not DNS), don't use != for this!	
	TCP or UDP port is 80 (HTTP)	
Properties-		
Filter name	: IP address 192.168.0.1	
Filter string	: ip.addr == 192.168.0.1	
<u><u>H</u>elp</u>		
Ready to load or capture		No Packets Profile: Def/

# **Display Filter Examples**

ip.src==10.1.11.24

ip.addr==192.168.1.10 && ip.addr==192.168.1.20

tcp.port==80 || tcp.port==3389

!(ip.addr==192.168.1.10 && ip.addr==192.168.1.20)

(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) && (tcp.port==445 || tcp.port==139)

(ip.addr==192.168.1.10 && ip.addr==192.168.1.20) && (udp.port==67 || udp.port==68)

#### **Protocol Hierarchy**

Tucker Ellis & West Obsolete_Packe	s.cap - Wireshark		
<u>File Edit View Go Capture Analyze</u>	<u>Statistics</u> <u>H</u> elp		
	Summary Protocol Hierarchy	77 业   🔳 📑   €	l Q @ 🖭 📓 🗹 🛛 🛨
<u>Filter:</u>	Dig Conversations	▼ Expression Clear App	ły
802.11 Channel: 🔹 Cha	Endpoints <u>I</u> O Graphs	Decryption I	Mode: None 🗸
No Time Source	Conversation List	Protocol	Info
1 0.000000 :: 2 0.000010 ::	Endpoint List Service Response Time	Od:56e3 ICMPv6 Od:56e3 ICMPv6	Multicast listener repo Multicast listener repo
3 2.179063 192.168.	ANSI +	255 NBNS	Name query NB LOCALHOST
5 2.715733 192.168.	🔕 Fax T38 Analysis	255 NBNS	Name query NB LOCALHOS
<u>6 2.821401 192.168.</u> 7 2.821546 192.168.	GSM ►	254 DNS 254 DNS	Standard query PTR 66.1 Standard query PTR 255.
8 2.824683 192.168. 9 2.990859 192.168.	G H.225 1 MTP3 ▶	66 DNS 03,255 NBNS	Standard query response
10 3.266913 192.168.	RTP •	03.255 NBNS	Name query NB LOCALHOST
12 3.495727 fe80::20	SCTP +	ICMPV6 ICMPV6	Router solicitation
13 3.542893 192.168. 14 3.543088 192.168.	A VolP Calls	254 DNS 03.255 NBNS	Standard query A DoCoMo Name querv NB LOCALHOSI
<b>T</b>	A WAP-WSP		
Frame 1 (88 bytes on wire, ■ Linux cooked capture	BOOTP-DHCP		
■ Internet Protocol Version	Destinations		
Internet Control Message P     ■	Flo <u>w</u> Graph HTTP		
	IP address		
	ISUP Messages Multicast Streams		
	ONC-RPC Programs		
	Packet Length		
	SMPP Operations		
0000 00 04 00 01 00 06 00 0 0010 60 00 00 00 00 20 00 0	TCP Stream Graph	aa).v	
0020 00 00 00 00 00 00 00 00 0030 00 00 00 01 ff 0d 56 e	3 3a 00 05 02 00 00 01	00v. :	···
0040 83 00 d2 c2 00 00 00 00 00 00 00 00 00 00 00 00 00	) ff 02 00 00 00 00 00	00	••••
File: "C:\Users\ro2.TEW\Downloads\Obsolete	Packets.cap_ Packets: 10949 Disp	layed: 10949 Marked: 0	Profile: Default

### **Protocol Hierarchy**

Mireshark: Protocol Hierarchy Statistics							<u> – D ×</u>
	Display fi	lter: none					
Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊡ Frame	100.00%	10949	1433310	0.004	0	0	0.000
Linux cooked-mode capture	100.00%	10949	1433310	0.004	0	0	0.000
Internet Protocol Version 6	0.16%	18	1392	0.000	0	0	0.000
Internet Control Message Protocol v6	0.16%	18	1392	0.000	18	1392	0.000
Internet Protocol	82.62%	9046	1312691	0.004	0	0	0.000
User Datagram Protocol	17.33%	1898	262866	0.001	0	0	0.000
Transmission Control Protocol	64.69%	7083	1046121	0.003	2350	163598	0.000
Internet Group Management Protocol	0.57%	62	3440	0.000	62	3440	0.000
Internet Control Message Protocol	0.03%	3	264	0.000	3	264	0.000
DEC DNA Routing Protocol	2.60%	285	14820	0.000	285	14820	0.000
Address Resolution Protocol	7.63%	835	46928	0.000	835	46928	0.000
MS Network Load Balancing	1.26%	138	8280	0.000	138	8280	0.000
Data	2.75%	301	25143	0.000	301	25143	0.000
Logical-Link Control	2.23%	244	20024	0.000	0	0	0.000
Appletalk Address Resolution Protocol	0.37%	40	2480	0.000	40	2480	0.000
	1.46%	160	14328	0.000	0	0	0.000
Datagram Delivery Protocol	0.40%	44	3216	0.000	0	0	0.000
	0.27%	30	1680	0.000	0	0	0.000
⊞ Banyan Vines IP	0.47%	52	2352	0.000	0	0	0.000

Close

# Follow TCP Stream

📶 Tucker Ellis & West http-ethereal-trace-1 - Wireshark	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> elp	
▋₩₩₩₩₩ □	D. 🖆 🎽 🖌 🗸
Eilter: (ip.addr eq 192.168.1.102 and ip.addr eq 128.1 - Expression Qear Apply	
802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: No	ne 🔻
No Time Source Destination Protocol Info	
7       4.675312       192.168.1.102       128.119.245.12       TCP       uniko         8       4.694429       128.119.245.12       192.168.1.1       Mark Packet (toggle)       Mark Packet (toggle)         10       4.694458       192.168.1.102       128.119.245       192.168.1.1         10       4.694450       192.168.1.102       128.119.245       192.168.1.1         11       4.77289       128.119.245.12       192.168.1.1       Apply as Filter         12       4.718993       128.119.245.12       192.168.1.1       Apply as Filter         13       4.724332       192.168.1.102       128.119.245       128.119.245         14       4.750366       128.119.245.12       192.168.1.1       Colorize Conversation Filter         15       4.859777       192.168.1.102       128.119.245       Colorize Conversation SCTP         Image: The state of	eypro > http [SYN] > unikeypro [SYN, ypro > http [ACK] ethereal-labs/lab: > unikeypro [ACK] 1.1 200 OK (text, favicon.ico HTTP/1 1.1 404 Not Found ypro > http [ACK] 
<ul> <li>Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af</li> <li>Internet Protocol, Src: 128.119.245.12 (128.119.245</li> <li>Transmission Control Protocol, Src Port: http (80),</li> <li>Print Show Packet in New Window</li> </ul>	5:23 (00:08:74:4f:36 (192.168.1.102) 27), seq: 0, Ack: 1,
4	► ►
0000       00       08       74       4f       36       23       00       06       25       da       af       73       08       00       45       00      to6# %sE.         0010       00       30       00       00       37       06       0c       36       80       77       f5       0c       0a      to6# %sE.         0020       01       66       00       37       06       0c       36       80       77       f5       0c       0a      to6# %sE.         0020       01       66       05       10       1f       6b       a6       54       91       f5       32       64       b2       70       12       .f.Pk.       T2d.p.         0030       16       d0       0a       21       00       00       20       40       01       04       02      !      !      !	
File: "C:\Traces\http-ethereal-trace-1" 4443 Bytes 00:00:06	Packets: 1 Profile: Def //

# Follow TCP Stream

#### red - stuff you sent

blue - stuff you get

A Follow TCP Stream	
_Stream Content	
GET /ethereal-labs/lab2-1.html HTTP/1.1	<u> </u>
Host: gaia.cs.umass.edu	
Netscape/7.01	
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/ plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1 Accept-Language: en-us, en;q=0.50 Accept-Encoding: gzip, deflate, compress;q=0.9 Accept-Charset: ISO-8859-1, utf-8;g=0.66, *;q=0.66	
Keep-Alive: 300	
Connection: keep-alive	
НТТР/1.1 200 ОК Date: Tue, 23 Sep 2003 05:29:50 GMT Server: Apache/2.0.40 (Red Hat Linux) Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT	
ETag: "1bfed-49-79d5bf00" Accept-Ranges: bytes	
Content-Length: 73	
Connection: Keen-Alive	
Content-Type: text/html; charset=ISO-8859-1	
<pre><ntml> Congratulations You've downloaded the file lab2-1 html!</ntml></pre>	
GET /favicon.ico HTTP/1.1	
HOST: gala.CS.umass.edu User_Agent: Mozilla/5 0 (Windows: U: Windows NT 5 1: en_US: rv:1 0 2) Cecko/20021120	
Netscape/7.01	
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/	
plain; q=0.8, video/x-mng, image/png, image/jpeg, image/gif; q=0.2, text/css, */*; q=0.1	
Accept-Language. en-us, en, q=0.30	
Find       Save As       Print       Entire conversation (2714 bytes)	Raw
Help Eiter Out Th	iis Stream

## Conversations

📶 Tucker Ellis & West http-ethereal-trac	e-1 - Wireshark	
<u>File Edit View Go Capture Analyze</u>	Statistics Help	
	Summary Protocol Hierarchy	7 ½ ■ 🖬 🕂 ੨ ལ 🖽 🖉 🔻
<u>Filter:</u>	Disconversations	▼ Expression Clear Apply
802.11 Channel: 🔹 Char	Endpoints <u>I</u> O Graphs	Decryption Mode: None
No Time Source	Conversation List	Protocol Info
2 0.017162 192.168.1	Service Response Time	102 SNMP get-response SNMPv2-SM;
<u>3 3.017086 192.168.1</u> 4 3 034572 192 168 1	ANSI 🕨	104 SNMP get-request SNMPv2-SMI 102 SNMP get-response SNMPv2-SMI
5 4.626878 192.168.1	🗛 Fax T38 Analysis	19 DNS Standard query A gaia.
6 4.663785 63.240.76	GSM 🔸	102 DNS Standard query response
8 4.694429 128.119.2	🗛 H.225	102 TCP http > unikeypro [SYN,
9 4.694458 192.168.1	MTP3	15.12 TCP unikeypro > http [ACK]
11 4.717289 128.119.2	RTP >	102 TCP http > unikeypro [ACK]
12 4.718993 128.119.2		102 HTTP HTTP/1.1 200 OK (text/
<u>13 4.724332</u> <u>192.168.1</u> 14 4.750366 <u>128.119.2</u>	G V-ID C-II-	102 HTTP GET /Tavicon.ico HTTP/1
<u>त</u>		
∃ Frame 2 (93 bytes on wire,	( WAP-WSP	
Ethernet II, Src: Hewlett-	BOOTP-DHCP	eb:ed), Dst: DellComp_4f:36:23 (00:08:74:4f:36
Internet Protocol, Src: 19     Internet Protocol, Src	Destinations	104), Dst: 192.168.1.102 (192.168.1.102)
∃ User Datagram Protocol, Sr	How Graph	Port: opsview-envoy (4125)
H SIMPLE NELWORK Management I	IP address	
	ISUP Messages	
	Multicast Streams	
	ONC-RPC Programs	
	Packet Length	
٩	Port Type SMPP Operations	<b></b>
0000 00 08 74 4f 36 23 00 30	TCP Stream Graph	00to6#.0 .aE.
0010 00 4T ec d8 00 00 3c 11 0020 01 66 00 a1 10 1d 00 3b	WLAN Traffic	as .0 <n 04 .f;01</n 
0030 06 70 75 62 6c 69 63 a2	24 02 02 18 31 02 01	00 .public. \$1
	01 00 04 01 10	v2
File: "C:\Traces\http-ethereal-trace-1" 4443 Byte	es 00:00:06	Packets: 1_ Profile: Def_ //

# Conversations

Conversations:	http-etherea	-trace-1							_	
Ethernet: 2 Fibre	Channel FDD	IPv4: 3	PX JXT	A NCP RSVP	SCTP TCP:	1 Token Ring	UDP: 4 USB	WLAN		
				IPv4 Co	onversations					
Address A	Address B	Packets +	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bp
63.240.76.19 192.168.1.102 128.119.245.12	192.168.1.102 192.168.1.104 192.168.1.102	2 6 9	370 555 3222	1 3 4	293 276 1956	1 3 5	77 279 1266	4.626878000 0.00000000 4.675312000	0.0369 6.0525 0.1845	N/ 36 84
4										▶
Name resolutio	n				🔲 Limit to d	isplay filter				
<u>H</u> elp								<u>С</u> ору	<u>C</u> lose	

# Flow Graphs

Tucker Ellis & West http-ethereal-trac	e-1 - Wireshark
<u>File Edit View Go Capture Analyze</u>	Statistics Help
	∑ Summary       Protocol Hierarchy
<u>F</u> ilter:	Dig Conversations
802.11 Channel: Char	Endpoints     IO Graphs     Ocryption Mode: None
No Time Source	Conversation List
1 0.000000 192.168.	Endpoint List 104 SNMP get-request SNMPV2-SMI
3 3.017086 192.168.	102 SNMP det-response SNMPV2-SM.
4 3.034572 192.168.	ANSI 102 SNMP get-response SNMPv2-SM1
5 4.626878 192.168.	Q Fax T38 Analysis 19 DNS Standard query A gaia.
6 4.663785 63.240.7	GSM 102 DNS Standard query response
8 4.694429 128.119.	$\bigcirc$ H.225 102 TCP http > unikeypro [SYN,
9 4.694458 192.168.	MTP3 + 5.12 TCP unikeypro > http [ACK]
10 4.694850 192.168.	RTP IS.12 HTTP GET /ethereal-labs/labi
	SCTP ID2 ICP NTTP > UNKeypro [ACK]
13 4.724332 192.168.	© SIP IS.12 HTTP GET /favicon.ico HTTP/1
14 4.750366 128.119.	♦ VolP Calls 102 HTTP HTTP/1.1 404 Not Found
4	MAD WSP
Protocol: UDP (0x11)	
⊞ Header checksum: 0x0da7	BOOTP-DHCP
Source: 192.168.1.104 (1	Destinations
Destination: 192.168.1.1	Flo <u>w</u> Graph
🖃 User Datagram Protocol, Sr	HTTP Port: opsview-envoy (4125)
Source port: snmp (161)	IP address
Destination port: opsvie	ISUP Messages
Length: 59	Multicast Streams
⊕ Checksum: 0x1ec4 [correc	ONC-RPC Programs
∃ Simple Network Management	Packet Length
<b> </b>	SMPB Operations
0000 00 08 74 4f 36 23 00 30	TCP Stream Grant 00 t06#.0 .aE.
0010 00 4f ec d8 00 00 3c 11	a8 .0 <hr style="text-align: center;"/> a8 .0
0030 06 70 75 62 6c 69 63 a2	24 02 02 18 31 02 01 00 .public. \$1
0040 02 01 00 30 18 30 16 00	5 11 2b 06 01 04 01 0b 020.0+
File: "C:\Traces\http-ethereal-trace-1" 4443 Bvt	es 00:00:06 Packets: 17 Displayed: 17 Marked: 0 Profile: Default

# Flow Graphs

Wireshark: Flo	Graph	<
Choose packets	Displayed packets	
Choose flow type <u>G</u> eneral flow	O ICP flow	
-Choose node add	ss type	
	QK <u>C</u> lose	

# Flow Graphs

🗖 http-e	thereal-trace-1 - Gr	raph Analysis				×
Time	192.168.1.102	192.168.1.104	63.240.76.19	128.119.245.12	Comment	<u></u>
0.000	(4125) get-request	SNMPv2			SNMP: get-request SNMPv2-SMI::enterprises.1	
0.017	det-response	e SNMPv2 (161)			SNMP: get-response SNMPv2-SMI::enterprises	
3.017	(4126) get-request	SNMPv2			SNMP: get-request SNMPv2-SMI::enterprises.1	
3.035	det-response	e SNMPv2			SNMP: get-response SNMPv2-SMI::enterprises	
4.627	(1026) S	tandard query A ga	►.(5.3)		DNS: Standard query A gaia.cs.umass.edu	
4.664	(1026) S	tandard query resp	(53)		DNS: Standard query response A 128.119.245.	
4.675	(4127)	unikeypro	> http [S		TCP: unikeypro > http [SYN] Seq=0 Win=64240	
4.694	(4127)	http > unik	eypro [S	(80)	TCP: http > unikeypro [SYN, ACK] Seq=0 Ack=	
4.694	(4127)	unikeypro	> http [A		TCP: unikeypro > http [ACK] Seq=1 Ack=1 Win	
4.695	(4127)	GET /ether	real-labs/		HTTP: GET /ethereal-labs/lab2-1.html HTTP/1.1	
4.717	(4127)	http > unik	eypro [A	(80)	TCP: http > unikeypro [ACK] Seq=1 Ack=502 W	
4.719	(4127)	HTTP/1.1 2	200 OK (t	(80)	HTTP: HTTP/1.1 200 OK (text/html)	
4.724	(4127)	GET /favic	on.ico HT		HTTP: GET /favicon.ico HTTP/1.1	
4.750	(4127)	HTTP/1.1 4	04 Not Fo	(80)	HTTP: HTTP/1.1 404 Not Found (text/html)	
4.860	(4127)	unikeypro	> http [A		TCP: unikeypro > http [ACK] Seq=989 Ack=172	
6.035	(4128) get-request	SNMPv2		1	SNMP: get-request SNMPv2-SMI::enterprises.1	
6.052	(4128) det-response	e SNMPv2			SNMP: get-response SNMPv2-SMI::enterprises	
[	4	1()		Þ	Image: The second se	-
		Save <u>A</u> s			Close	

# Assignment 3 – Understanding Network Traffic using Wireshark

- Deadline Sunday Feb 22, 11:59 PM
  - 1 bonus point for submission 24 hours before deadline
  - Firm deadline -> Start early

## Understanding Network Traffic using Wireshark

• Download the trace files, open with Wireshark and answer Q1-12 accordingly

- Q13 requires a real capture
  - Install Wireshark on your own machine

### Next lecture

- TCP
  - Readings 3.5
- Guest lecture on Monday Feb 23<sup>rd</sup>
   DNS Security
- Midterm exam in 4 weeks

– In class: 1 PM Friday, March 6<sup>th</sup>