Анализ трафика телефона

Программа **Wireshark** предназначена для снятия трафика. Основным её достоинством является наглядность анализируемых данных. Существуют различные топологии систем, которым может потребоваться анализ трафика.

В данном примере рассматривается настройка следующего вида: телефон DPH-120 (это может быть любой другой телефон серии D-Link аппаратной ревизий F3 и выше), который подключен к роутеру через WAN-порт и к сетевой карте компьютера через LAN-порт. При этом на телефоне и на сетевой карте компьютера настроены следующие параметры:

	Телефон	Сетевая карта		
IP-адрес	192.168.8.1	192.168.8.2		
Сетевая маска	255.255.255.0	255.255.255.0		
Шлюз	192.168.8.254	192.168.8.254		
Первичный DNS	8.8.8.8	8.8.8.8		
Вторичный DNS	8.8.4.4	8.8.4.4		

Стоит отметить, что адрес роутера совпадает с адресом шлюза настроек сетевой карты и телефона. Подключены между собой устройства таким образом, как показано на изображении:



Чтобы настроить зеркалирование портов, заходим на страницу настройки телефона DPH-120 в пункт меню NETWORK — LAN, и там отмечаем галочками поля Port Mirror и Enable Bridge Mode:

Firmware Version:2.5.573.84									
D-Link									
DPH-120SE	BASIC	NETWORK	VoIP	PHONE	FUNCTION KEY	MAINTENANCE	SECURITY		
WAN LAN	LAN Settin	gs የ							
QoS&VLAN	IP Address Subnet Mask		192.168.1 255.255.2	0.1 55.0					
SERVICE PORT	DHCP Service								
DHCP SERVICE	NAT								
TIME&DATE	Port Mirror		🗹 (Only)	works in the br	idge mode!)				
	Enable Bridge	Mode							
			Apply						
BROADBAND									
Copyright © 2010 D-Link International Pte. Ltd.									

После указанных действий внизу нужно применить изменения, нажав кнопочку Apply. Когда эти действия будут завершены, зайти в раздел MAINTANCE — REBOOT и нажать кнопочку Reboot для перезагрузки и корректного сохранения данных.

Теперь для получения трафика необходимо открыть предварительно установленную программу Wireshark, щёлкнуть по кнопке Capture Options и выбрать интерфейс, с которого будет производиться снятие данных. В рассматриваемом случае это интерфейс сетевой карты enp5s0. После выбора, нажать внизу кнопочку Start.

affic Lin Lin Ett Lin Ra un un un un un	ik-layer Header hux cooked hernet hernet ux netfilter log messages w IPv4 known known known	Promiscuous enabled enabled enabled enabled enabled enabled enabled	Snaplen (default default default default default default default	Buffer (M 2 2 2 2 2 2 2 2 2	Monitor Moi Captur n/a n/a n/a n/a n/a n/a	e Filter	
Lin Ett Lin Ra un un un un	nux cooked hernet hernet ux netfilter log messages w IPv4 known known known	enabled enabled enabled enabled enabled enabled enabled	default default default default default default	2 2 2 2 2 2 2	n/a n/a n/a n/a n/a		
Et Eti Lin Ra un un un un	hernet hernet ux netfilter log messages w IPv4 known known known	enabled enabled enabled enabled enabled enabled	default default default default default default	2 2 2 2 2	n/a n/a n/a n/a		
Et Lin Ra un un un	hernet 1ux netfilter log messages 1w IPv4 known known known	enabled enabled enabled enabled enabled	default default default default default	2 2 2 2	n/a n/a n/a n/a		
Lin Ra un un un un	iux netrilter log messages w IPv4 known known known	enabled enabled enabled enabled	default default default default	2 2 2	n/a n/a n/a		
Ka un un un	w 1274 known known known	enabled enabled enabled	default default default	2	n/a n/a		
un un un un	known known known	enabled	default	2	n/a		
un un un	known	enabled	OPLAUIT	2	n/n		
un	KIIOWII	opphlod	dofault	2	n/a		
un	known	enabled	default	2	n/a		
lin	known	enabled	default	2	n/a		
un	known	enabled	default	2	n/a		
un	known	enabled	default	2	n/a		
un	known	enabled	default	2	n/a		
un	known	enabled	default	2	n/a		
ous mode on all interfac	ces					Ma	anage Interfaces
5	un un un us mode on all interfa	unknown unknown unknown us mode on all interfaces	unknown enabled unknown enabled unknown enabled us mode on all interfaces	unknown enabled default unknown enabled default unknown enabled default us mode on all interfaces	unknown enabled default 2 unknown enabled default 2 unknown enabled default 2 us mode on all interfaces	unknown enabled default 2 n/a unknown enabled default 2 n/a unknown enabled default 2 n/a unknown enabled default 2 n/a	unknown enabled default 2 n/a unknown enabled default 2 n/a unknown enabled default 2 n/a ws mode on all interfaces

Для удобства, в верхнем окне программы Wireshark стоит выбрать протокол анализируемого трафика. Т.к. в данном примере рассматривается сигнальный VoIP трафик, выберем протокол SIP.



В случае, если всё будет настроено правильно, при звонке с этого телефона, в окне программы Wireshark появится строки следующего вида:

<u>File</u>	dit View Go Capture	Analyze Statistics T	elephony <u>W</u> ireless <u>T</u> o	ols <u>H</u> elp			
	1 🔘 🚞 🛅	🗙 🙆 🔍 🦛 🗉	🔶 🕮 🟹 🔶 📃	$\square \oplus \oplus \oplus \blacksquare$			
cin							Tunnessian t
	7	C	Bestleytley	Protocol Longth	1-6-		Expression +
NO.	9 / 206257932	192 168 8 1	192 168 8 254	STP Length	AAA Pequest: CANCEL sin:8010192 168	8 254 user=nhone	
	10 4.211911910	192.168.8.254	192.168.8.1	SIP	403 Status: 487 Request Terminated		
	11 4.212610765	192.168.8.254	192.168.8.1	SIP	387 Status: 200 OK		
L	12 4.217745519	192.168.8.1	192.168.8.254	SIP	383 Request: ACK sip:801@192.168.8.3	254;user=phone	
▶ Fra	me 9: 409 bytes on	wire (3272 bits), 409 bytes capt	ured (3272 bits) o	n interface 0		
▶ Eth	ernet II, Src: 00:	a8:59:d8:7b:72 (00:a8:59:d8:7b:72	2), Dst: D-LinkIn_7	2:67:d7 (70:62:b8:72:67:d7)		
▶ Int	ernet Protocol Ver	sion 4, Src: 192	.168.8.1, Dst: 19	2.168.8.254			
► Use	r Datagram Protoco.	1, Src Port: 506	0 (5060), Dst Por	t: 5060 (5060)			
P Ses	STON THICIALION PR	ULUCUI (CANCEL)					
0000	70 62 b8 72 67 d7	00 a8 59 d8 7b	72 08 00 45 00	pb.rg Y.{rE.			-
0010	01 8b 00 27 00 00	40 11 e6 eb c0	a8 08 01 c0 a8	'@			
0020	08 fe 13 c4 13 c4	01 77 a6 3f 43	41 4e 43 45 4c				
0030	20 /3 09 /0 3a 38	30 31 40 31 39 3b 75 73 65 73	32 20 31 30 38	Sip:801 @192.168			
0040	26 30 26 32 33 34	30 13 13 03 12	. 30 70 00 01 0e	.0.204,0 Set-phon			*
0 7	wireshark_pcapng_enp5s	0 20170605152349 yct	:TDj			Packets: 137 · Displayed: 4 (2.9%)	Profile: Default