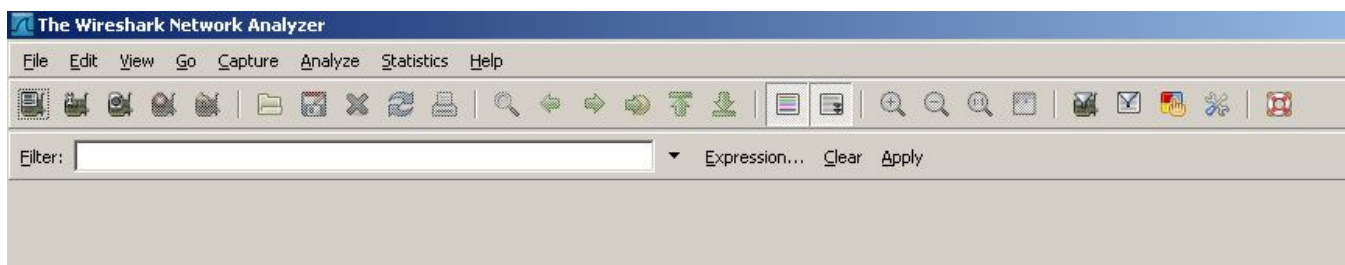
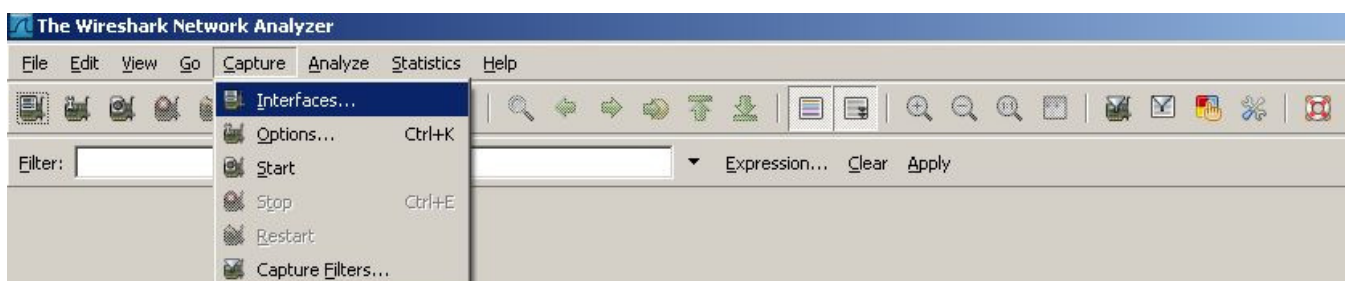


Procedimento para utilização do Wireshark para captura de pacotes TCP/IP

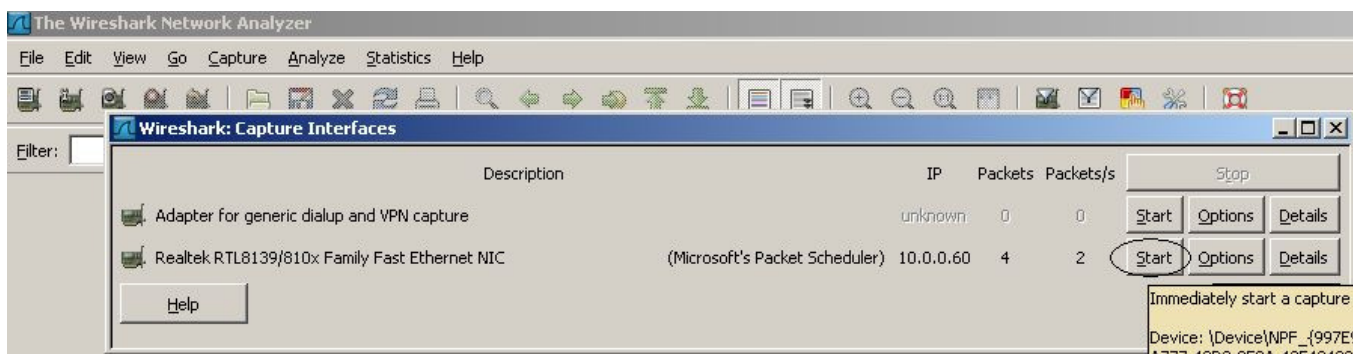
1º) Fazer a instalação na máquina que se comunica com o Inner:



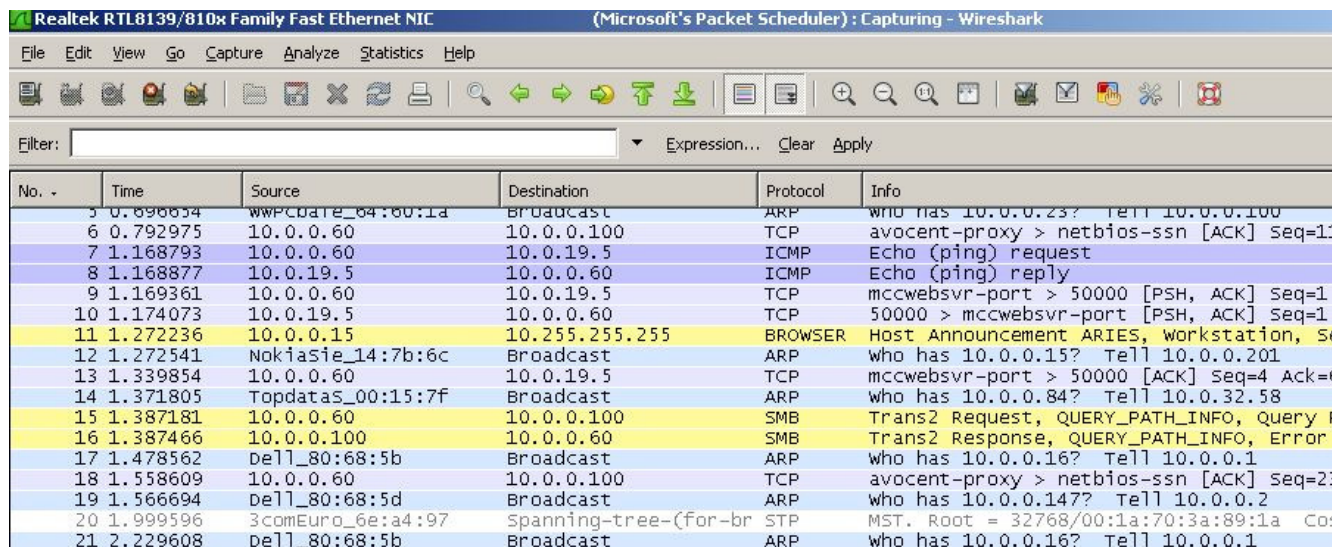
2º) Clicar em **Capture | Interfaces**



3º) Clicar em **"Start"** na interface de rede utilizada:

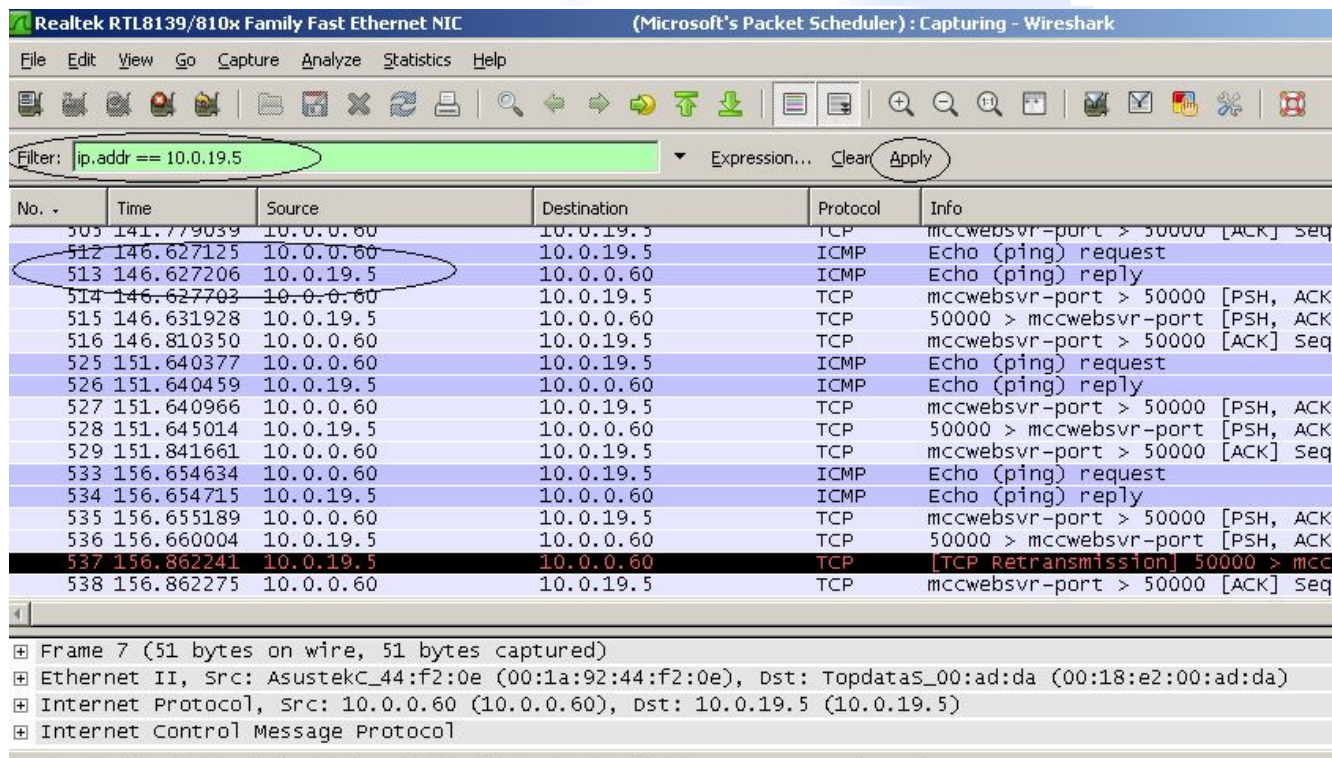


4º) Começará a fazer monitoração:



No. -	Time	Source	Destination	Protocol	Info
5	0.898654	WPCoarte_04:00:1a	Broadcast	ARP	who has 10.0.0.23? Tell 10.0.0.100
6	0.792975	10.0.0.60	10.0.0.100	TCP	avocent-proxy > netbios-ssn [ACK] Seq=1
7	1.168793	10.0.0.60	10.0.19.5	ICMP	Echo (ping) request
8	1.168877	10.0.19.5	10.0.0.60	ICMP	Echo (ping) reply
9	1.169361	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [PSH, ACK] Seq=1
10	1.174073	10.0.19.5	10.0.0.60	TCP	50000 > mccwebsvr-port [PSH, ACK] Seq=1
11	1.272236	10.0.0.15	10.255.255.255	BROWSER	Host Announcement ARIES, workstation, S
12	1.272541	Nokiasie_14:7b:6c	Broadcast	ARP	who has 10.0.0.15? Tell 10.0.0.201
13	1.339854	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [ACK] Seq=4 Ack=
14	1.371805	Topdatas_00:15:7f	Broadcast	ARP	who has 10.0.0.84? Tell 10.0.32.58
15	1.387181	10.0.0.60	10.0.0.100	SMB	Trans2 Request, QUERY_PATH_INFO, Query P
16	1.387466	10.0.0.100	10.0.0.60	SMB	Trans2 Response, QUERY_PATH_INFO, Error
17	1.478562	Dell_80:68:5b	Broadcast	ARP	who has 10.0.0.16? Tell 10.0.0.1
18	1.558609	10.0.0.60	10.0.0.100	TCP	avocent-proxy > netbios-ssn [ACK] Seq=2
19	1.566694	Dell_80:68:5d	Broadcast	ARP	who has 10.0.0.14? Tell 10.0.0.2
20	1.999596	3comEuro_6e:a4:97	Spanning-tree-(for-br	STP	MST. Root = 32768/00:1a:70:3a:89:1a Cos
21	2.229608	Dell_80:68:5b	Broadcast	ARP	who has 10.0.0.16? Tell 10.0.0.1

5º) Colocar um filtro no Wireshark, com o endereço IP do Inner a ser diagnosticado, por exemplo, "ip.addr == 10.0.19.5"



No. -	Time	Source	Destination	Protocol	Info
505	141.779039	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [ACK] seq
512	146.627125	10.0.0.60	10.0.19.5	ICMP	Echo (ping) request
513	146.627206	10.0.19.5	10.0.0.60	ICMP	Echo (ping) reply
514	146.627703	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [PSH, ACK
515	146.631928	10.0.19.5	10.0.0.60	TCP	50000 > mccwebsvr-port [PSH, ACK
516	146.810350	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [ACK] Seq
525	151.640377	10.0.0.60	10.0.19.5	ICMP	Echo (ping) request
526	151.640459	10.0.19.5	10.0.0.60	ICMP	Echo (ping) reply
527	151.640966	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [PSH, ACK
528	151.645014	10.0.19.5	10.0.0.60	TCP	50000 > mccwebsvr-port [PSH, ACK
529	151.841661	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [ACK] Seq
533	156.654634	10.0.0.60	10.0.19.5	ICMP	Echo (ping) request
534	156.654715	10.0.19.5	10.0.0.60	ICMP	Echo (ping) reply
535	156.655189	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [PSH, ACK
536	156.660004	10.0.19.5	10.0.0.60	TCP	50000 > mccwebsvr-port [PSH, ACK
537	156.862241	10.0.19.5	10.0.0.60	TCP	[TCP Retransmission] 50000 > mcc
538	156.862275	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [ACK] Seq

Frame 7 (51 bytes on wire, 51 bytes captured)
 Ethernet II, Src: AsustekC_44:f2:0e (00:1a:92:44:f2:0e), Dst: Topdatas_00:ad:da (00:18:e2:00:ad:da)
 Internet Protocol, Src: 10.0.0.60 (10.0.0.60), Dst: 10.0.19.5 (10.0.19.5)
 Internet Control Message Protocol

6º) Reproduzir a situação desejada.

7º) Salvar o log

Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet Scheduler) : Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Open... Ctrl+O
Open Recent
Merge...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export
Print... Ctrl+P
Quit Ctrl+Q

No.	Time	Source	Destination	Protocol	Info
3362	38.472876	10.0.0.60	Spanning-tree-(for-br	STP	MST. Root = 32768/00:1a:70:3a:89:1a Cost = 20
3363	38.472883	10.0.0.60	10.0.19.5	TCP	mccwebsvr-port > 50000 [PSH, ACK] Seq=22 Ack=37
3364	38.472992	10.0.0.100	10.0.0.100	TCP	50000 > mccwebsvr-port [PSH, ACK] Seq=37 Ack=2
3365	38.473035	10.0.0.100	10.0.0.60	TCP	neon24x7 > navbuddy [ACK] Seq=319 Ack=408 win=
3366	38.473047	10.0.0.60	10.0.0.100	TCP	navbuddy > neon24x7 [ACK] Seq=408 Ack=320 win=
3367	39.088241	WwPcbaTe_64:60:1a	Broadcast	ARP	who has 10.0.0.16? Tell 10.0.0.100
3368	39.672675	3comEuro_6e:a4:97	Spanning-tree-(for-br	STP	MST. Root = 32768/00:1a:70:3a:89:1a Cost = 20

Frame 1 (60 bytes on wire, 60 bytes captured)
 Ethernet II, Src: WwPcbaTe_64:60:1a (00:0f:1f:64:60:1a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (request)