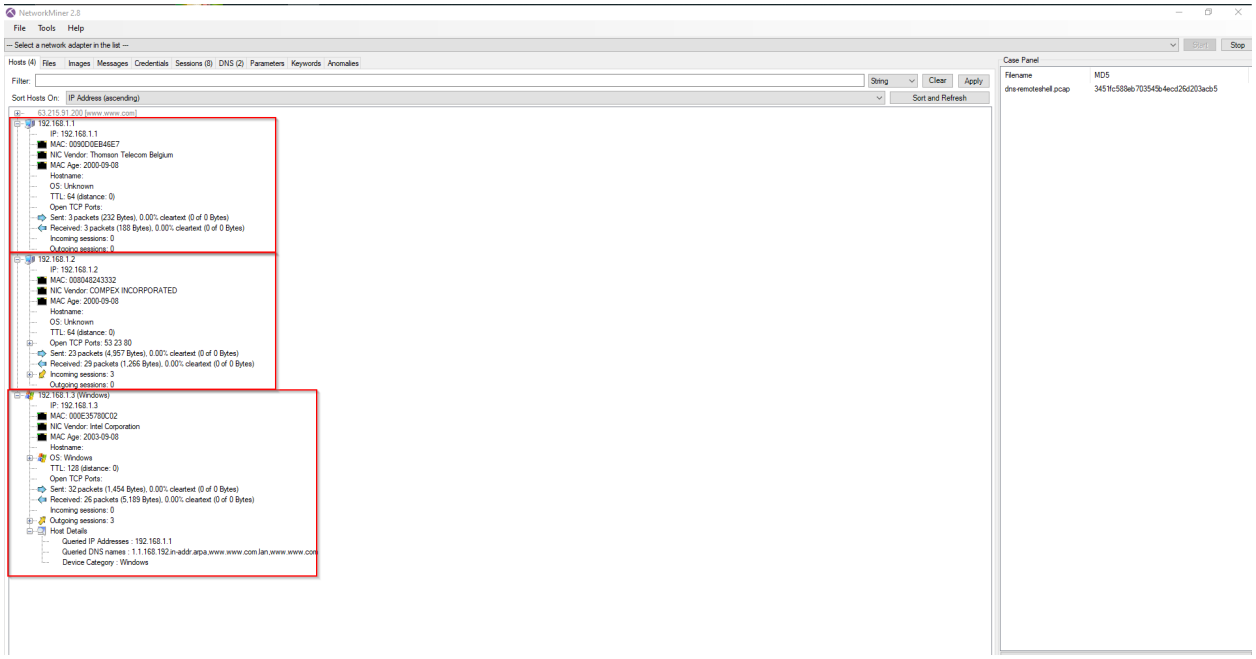
Packet Hunting:

Here we will do packet hunting, here will learn how to use our proposed methodology(things we learned so far) to perform packet hunt. We will be using tools like Wireshark, Network miner:

We will be looking at PCAP where we will hunt for Remote Shell that uses port 53 for the C2 connection. Its common for attackers to use the open ports as part of the C2 connection as the port is already open.

First we will open this PCAP in network miner to get an overview of the PCAP:

First we will look at the HOST tab to get a good overview of the machines and then sport anything out of the ordinary like we see a Web server creates a outgoing session which it shouldn't as it wait for connection, mean it waits for incoming sessions:

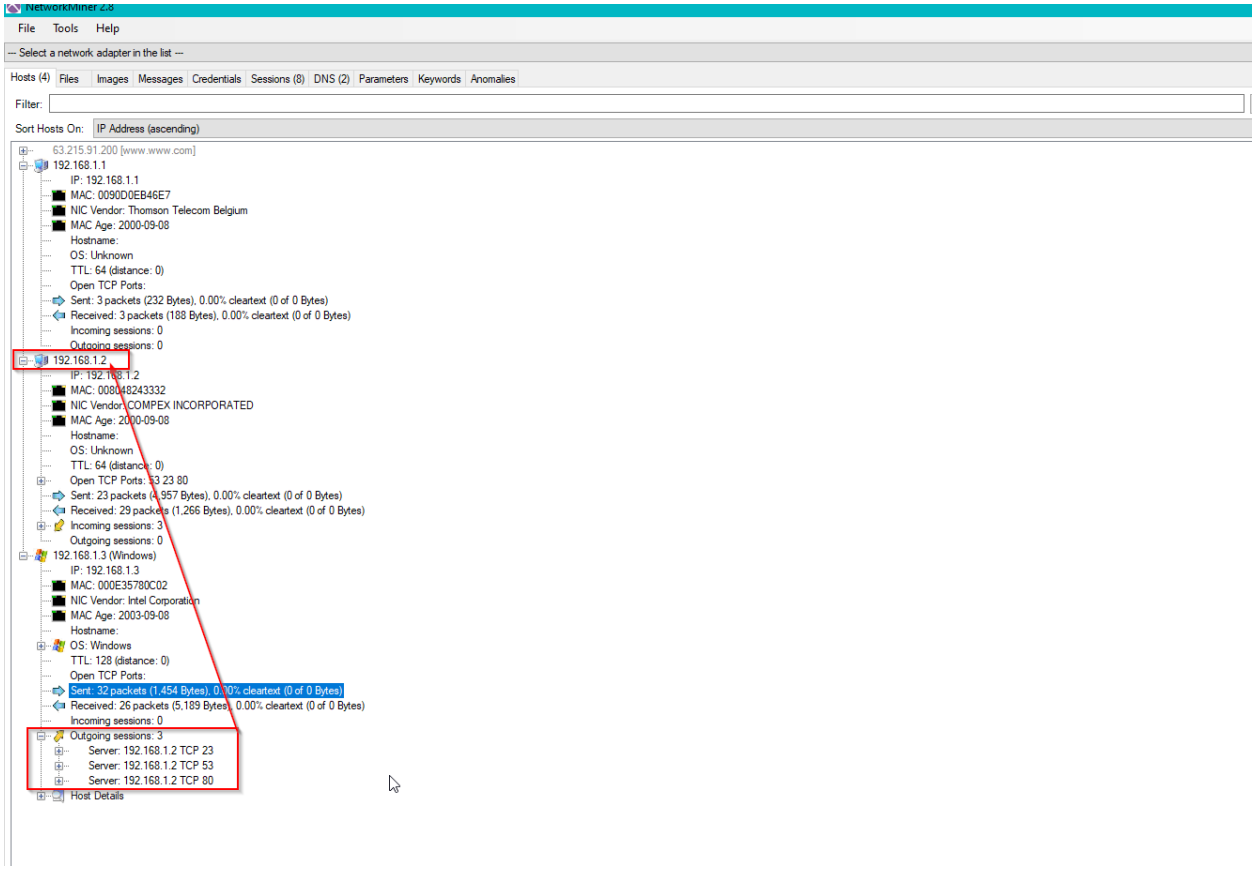


Here we see the first 2 Hosts OS is unknow but the 3rd one is Windows, the first one and the last one dosnt have any port open, but the second host 192.168.1.2 has port 53,23 and 80 open which indicates it's a Server and we also see the Incoming sessions, mean its listening for connection. The 3rd host has 3 outgoing sessions and we also see it has Host Details which much cant understand it yet.

The 1st host

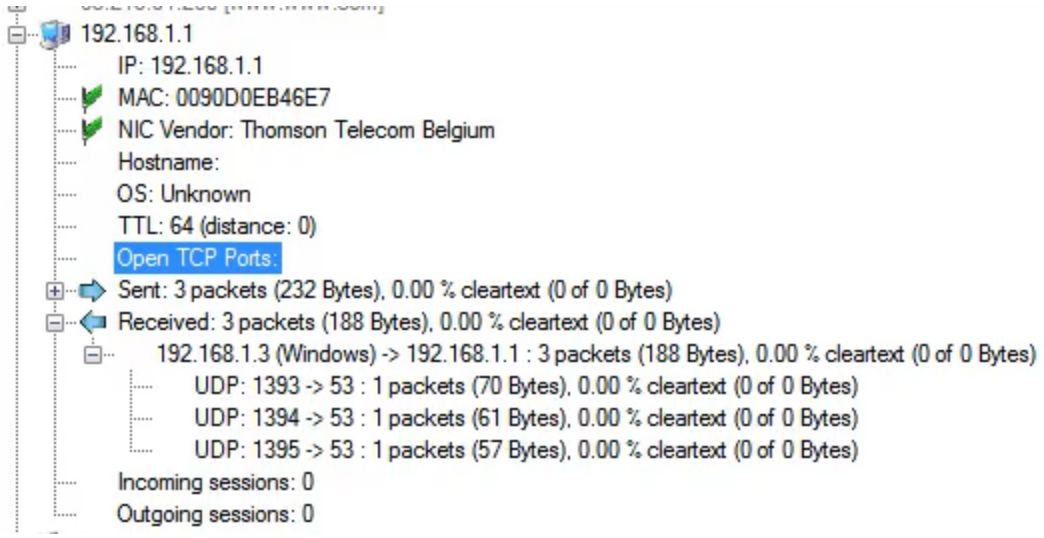
The first Host dosnt have any Session created.

Lets look at the 3rd host, 192.168.1.3 sessions:



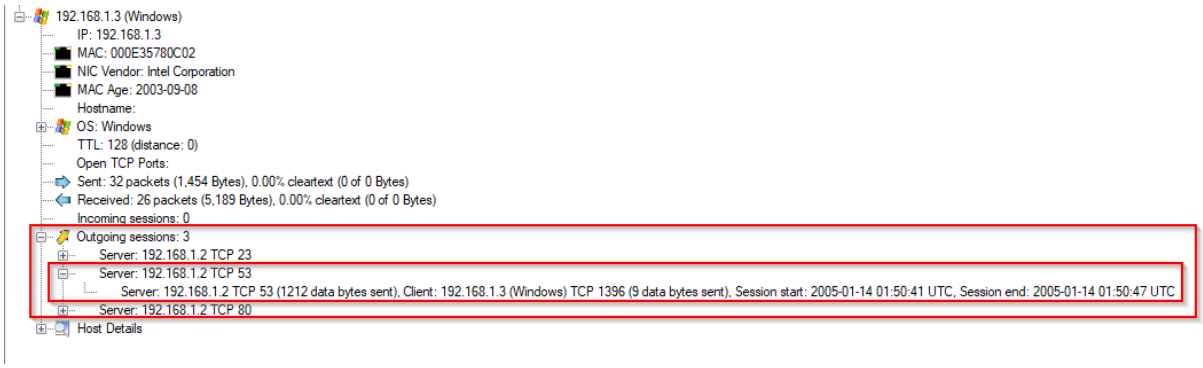
We see the 3rd host created 3 sessions and all of them are with the 2nd host over its all open ports, mean the 3rd host accessed all the ports of the 2nd host, the port 23,53 and 80. It connected successfully and created sessions with it: but one thing that is suspicious would be that the port 53 is TCP not UDP when the session is created:

For the 1st Host 192.168.1.1, there are no Session created, but it has received 3 packets and also sent 3 packets:



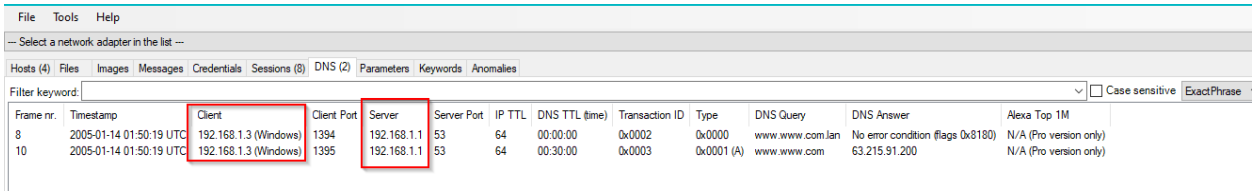
It received the 3 packets from the 3rd host 192.168.1.3 over its port 53 UDP, mean the host 1st 192.168.1.1 opened port 53 UDP and then the 3rd host 192.168.1.3 send 3 packets to the 1st host.

Lets go back to the outgoing sessions of the 3rd host 192.168.1.2 and look at it:



As we said it has TCP over the port 53 and it's a Red flag. The only reason that TCP would be used for DNS is when the date is to large to fit in the UDP Packet so the TCP packet will be used:

Lets find this out, why this port is used, in the Network Miner we see the DNS tab, lets go to it:

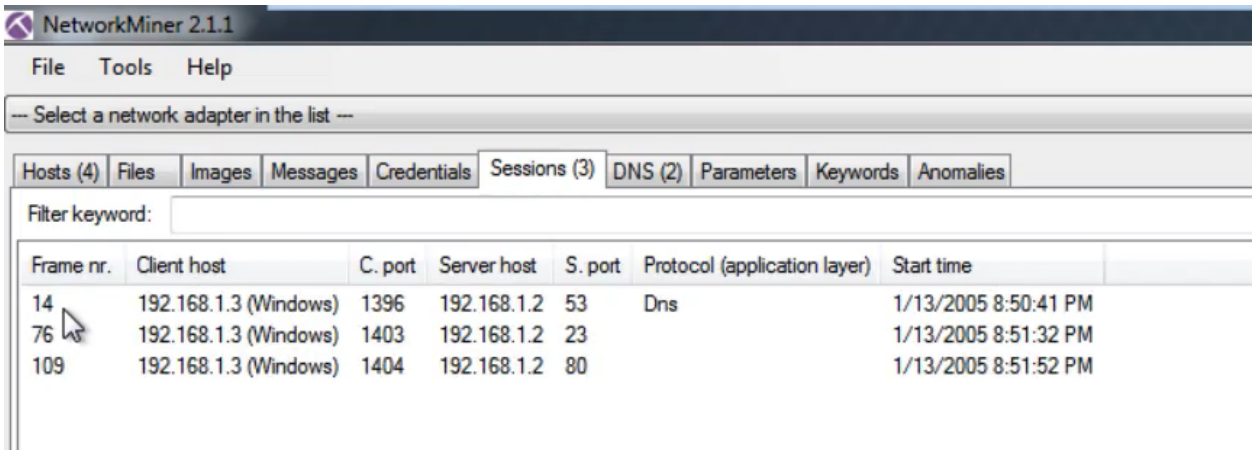


In the DNS Tab we see the Traffic from Host 3 to host 1 over port 53 UDP, which is strange it self as we said before when we were examining the Host tab where we saw the Host 1 received UDP traffic over port 53 which means the 1st 192.168.1.1 host opened Port 53 and then it received the 3 packets from the 3 host but the 1st host is not a server as we saw on the Host tab it had no Port opened but here we see the 1st host received packets form the 3 host over port 53 UDP.

And we also don't see the TCP traffic from host 3 to the host 2 over port 53 TCP and that's suspicious

So we have 2 Red Flags so far:

Lets go to the session TAB:

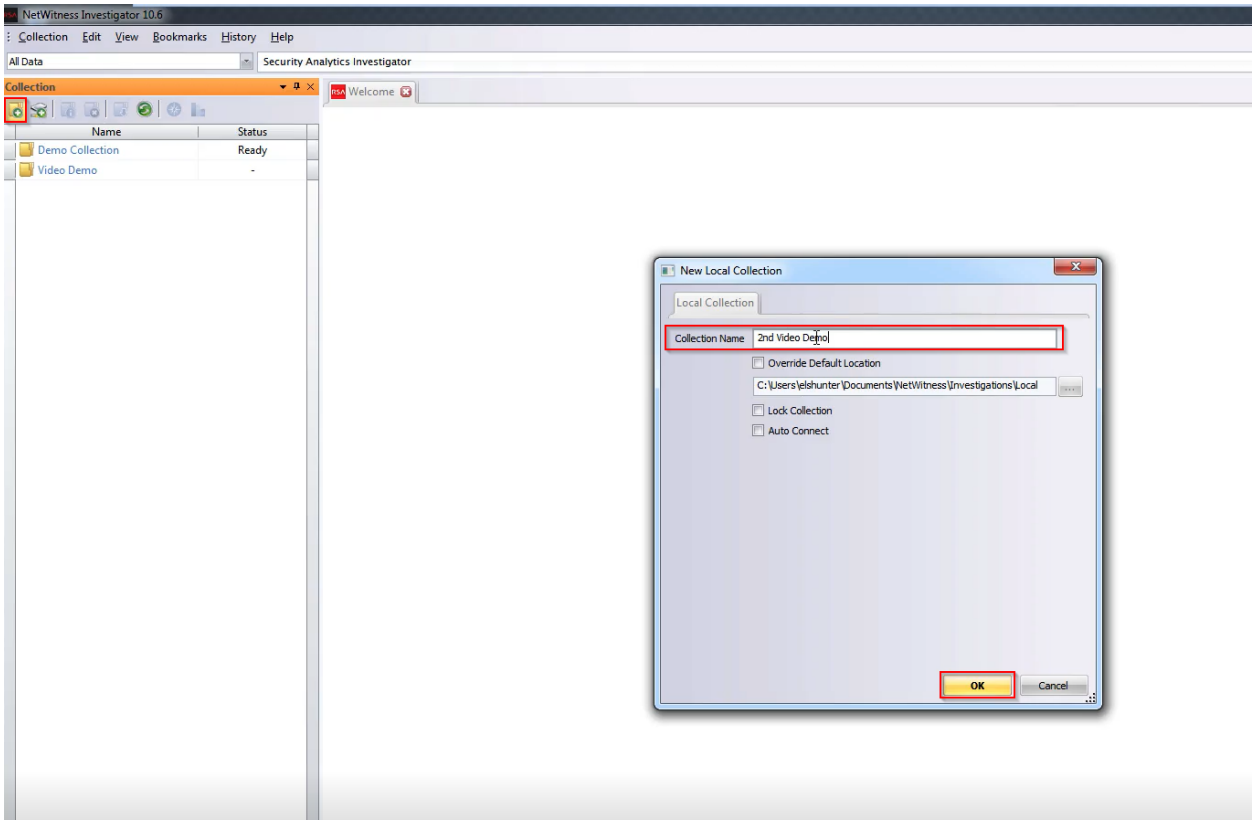


We see the Host 3, 3 outgoing Sessions, that's the only sessions we had when we checked the Host Tab, and here again we see the traffic from host 3rd 192.168.1.3 to host 2nd 192.168.1.2, and we know the 2nd host 192.168.1.2 have port 53 open but its only UPD but as we saw in the Host tab the traffic between these 2 host is Over TCP not UDP which makes is suspicious.

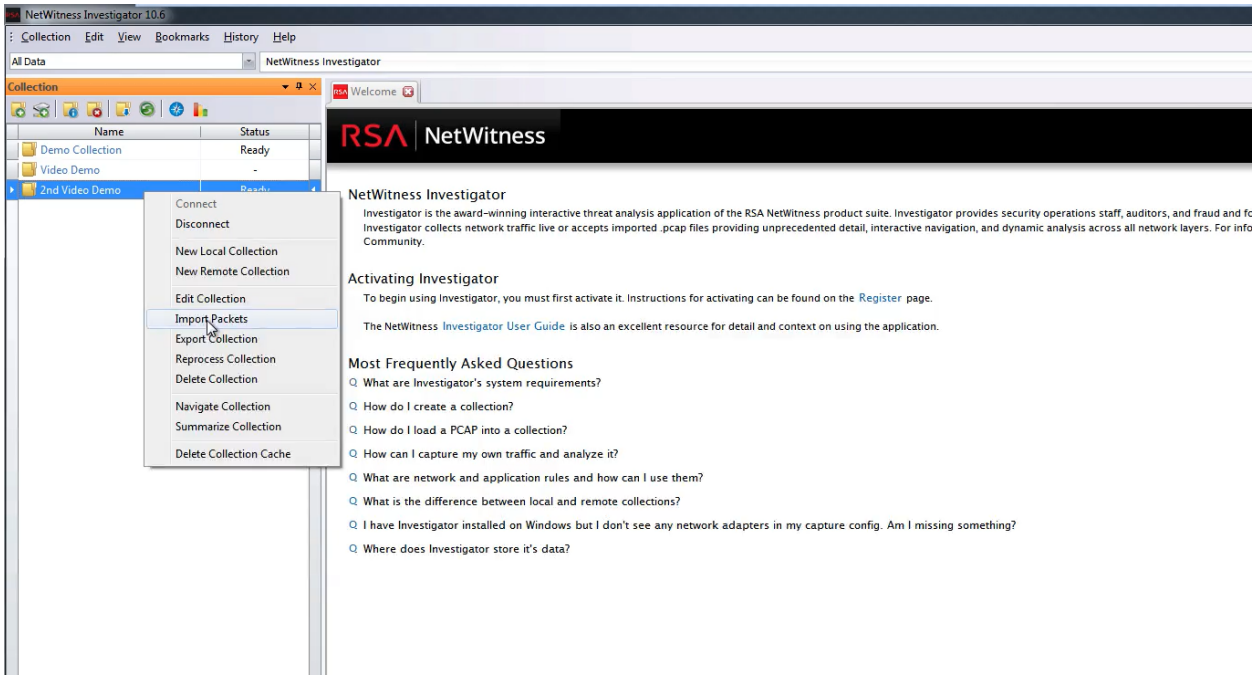
Dost that mean the 3rd host is masking its traffic by using port 53?

Lets open the pcap in NetWitness Investigator:

First we need to start a new collection for this New PCAP file, we click the New collection, put its name and click ok:



We right click it to connect this collection and then we right click it again to import the PCAP file:



Select the PCAP file the Directory and double click the collection:

NetWitness Investigator 10.6

Collection Edit View Bookmarks History Help

All Data | 2nd Video Demo

2nd Video Demo

< 2005-01-13 20:50

Service Type (4 items)
DNS (3) - OTHER (3) - FTP (2) - SSL (1)

Hostname Aliases (1 item)
www.www.com (1)

Source IP Address (1 item)
192.168.1.3 (8)

Destination IP address (2 items)
192.168.1.2 (5) - 192.168.1.1 (3)

TCP Destination Port (4 items)
21 (ftp) (2) - 80 (http) (1) - 53 (domain) (1) - 23 (telnet) (1)

UDP Target Port (1 item)
53 (domain) (3)

Ethernet Protocol (2 items)
IP (8) - ARP (1)

IP Protocol (2 items)
TCP (5) - UDP (3)

Crypto (2 items)
tls_rsa_with_rc4_128_md5 (1) - ssl 3.0 (1)

Ethernet Source (1 item)
00:0E:35:78:0C:02 (9)

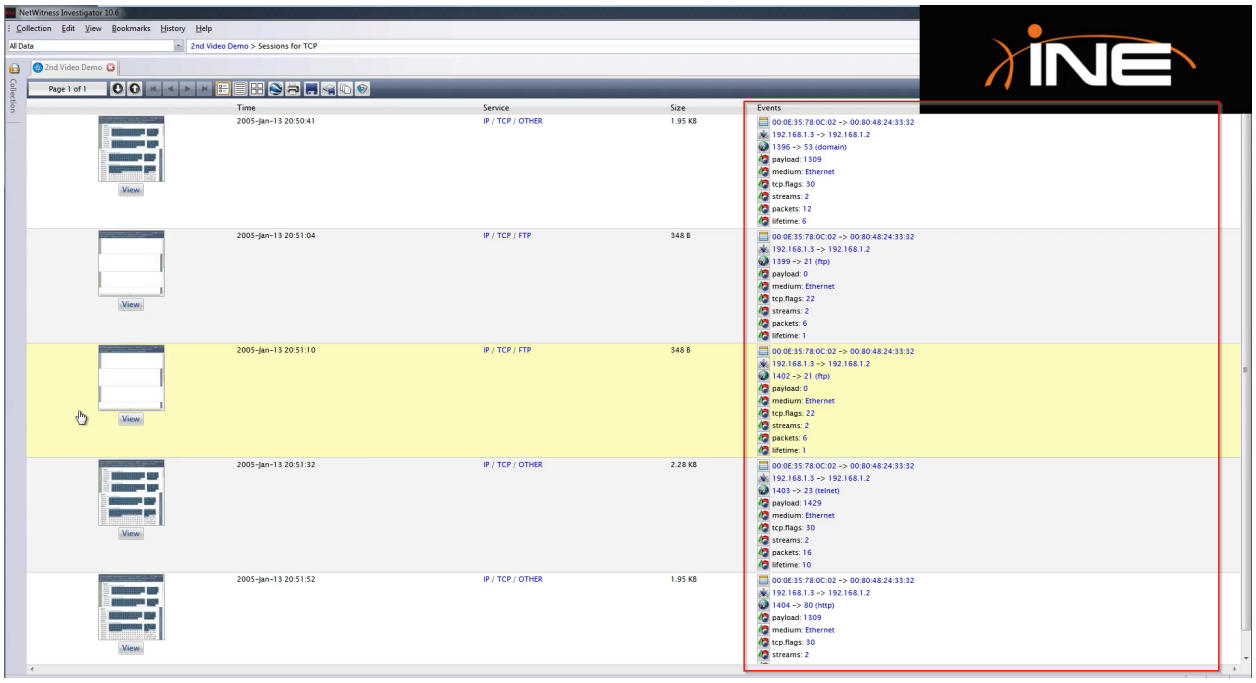
Ethernet Destination (3 items)
00:80:48:24:33:32 (5) - 00:90:D0:EB:46:E7 (3) - FF:FF:FF:FF:FF:FF (1)

IP Aliases [open]

Alert ID (1 item)
nw125015 (1)

Here first we see the Service Type which shows all the protocols within the Packet. And in the TCP Destination port we see all the Destination ports.

And in the IP protocol we see TCP and UDP, which shows the Transport protocols: lets click the TCP under it: and we see it has 5, which means if we click the TCP we will see the 5 packets and its details:

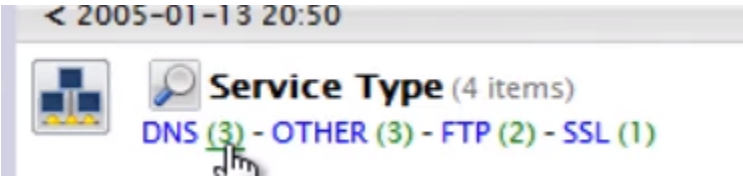


Here we see the details of it to the right of each packet: we can look at the Packet details, but its better to do that in Wireshark:

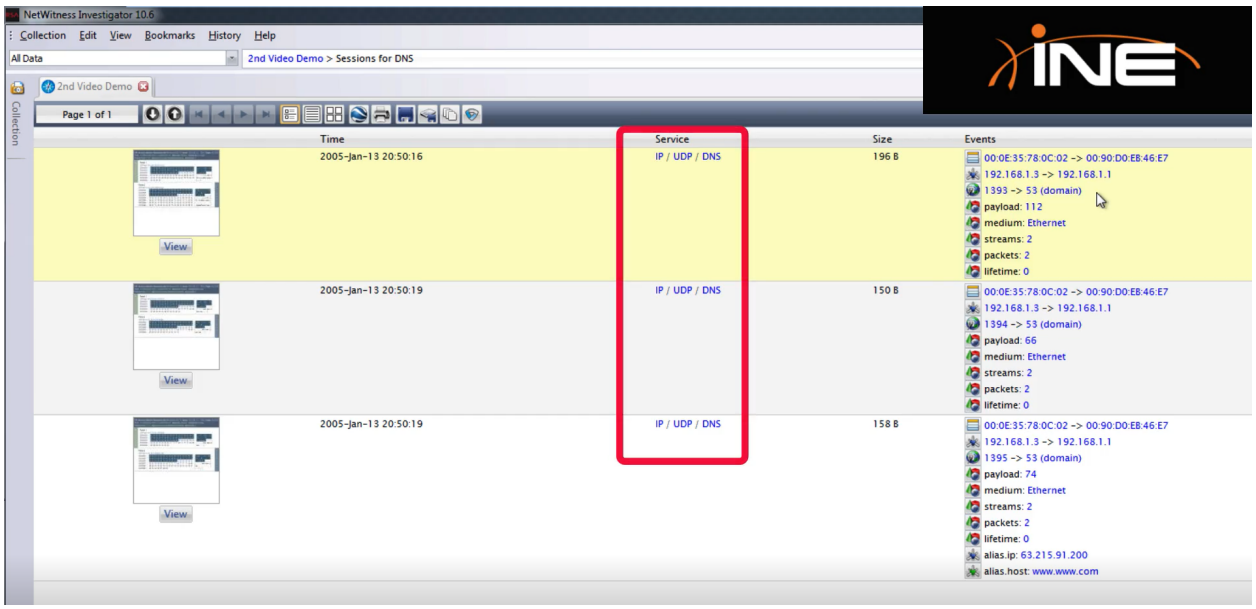
Now lets go back and then click on the TCP Destination port under port 53 domain:

We will see the same information, the 3rd 192.168.1.3 host from the network miner is communicated over TCP port 53 of the 2nd host 192.168.1.2 . its TCP here as we see under the Service we see IP / TCP.

Lets just look at the DNS traffic under the Service Type, we will click the DNS:



The traffic:



As we saw in the network miner, we saw that port 53 UDP was open on host 1st 192.168.1.1 and then the 3rd host 192.168.1.3 sent through it to the host 1, 3 packets. we see the same thing here.

So far in both of the tools we confirmed the 2 red flags:

Lets open the Same PCAP in Wireshark:

Lets look at the PCAP protocol hierarchy:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	131	100.0	22885	1835	0	0	0	131
Ethernet	100.0	131	8.6	1957	156	0	0	0	131
Internet Protocol Version 4	94.7	124	10.8	2480	198	0	0	0	124
User Datagram Protocol	4.6	6	0.2	48	3	0	0	0	6
Domain Name System	4.6	6	1.1	252	20	6	252	20	6
Transmission Control Protocol	90.1	118	66.4	15192	1218	104	11881	953	118
Transport Layer Security	2.3	3	3.9	887	71	3	887	71	3
Telnet	6.1	8	6.2	1429	114	8	1429	114	8
Hypertext Transfer Protocol	1.5	2	3.1	713	57	2	713	57	2
Data	0.8	1	0.0	2	0	1	2	0	1
IEEE 802.11 wireless LAN	52.7	69	7.2	1656	132	0	0	0	69
Logical-Link Control	52.7	69	52.3	11965	959	0	0	0	69
Address Resolution Protocol	5.3	7	1.0	232	18	7	232	18	7

We see most of the packets are TCP which is 118 packets and only 6 of them are UDP and we know that 3 of them are send by Host 3rd to the host 1st:

Lets look at conversation to see which host communicated to which host:

Wireshark · Conversations · dns-remoteshell.pcap

Conversation Settings
- Name resolution
- Absolute start time
- Limit to display filter

Ethernet · 6 | IPv4 · 5 | IPv6 | TCP · 9 | UDP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.2	1108	83.170.75.178	80	5	3.311 KiB	5	2	188 bytes	3	3.127 KiB	73.102744	0.0161	93 kbps	1595 kbps
192.168.1.2	1110	83.170.75.178	80	5	1.171 KiB	6	3	686 bytes	2	513 bytes	73.147503	0.0294	186 kbps	139 kbps
192.168.1.2	1026	140.112.253.189	22604	1	96 bytes	0	1	96 bytes	0	0 bytes	1.116040	0.0000		
192.168.1.3	1396	192.168.1.2	53	24	4.349 KiB	1	14	1.071 KiB	10	3.277 KiB	25.493358	5.3120	1652 bits/s	5054 bits/s
192.168.1.3	1399	192.168.1.2	21	12	936 bytes	2	6	492 bytes	6	444 bytes	48.475089	0.9755	4034 bits/s	3641 bits/s
192.168.1.3	1402	192.168.1.2	21	12	936 bytes	4	6	492 bytes	6	444 bytes	53.685910	0.9733	4043 bits/s	3649 bits/s
192.168.1.3	1403	192.168.1.2	23	33	5.267 KiB	7	18	1.380 KiB	15	3.887 KiB	75.776641	9.7935	1154 bits/s	3251 bits/s
192.168.1.3	1404	192.168.1.2	80	23	4.257 KiB	8	13	1,003 bytes	10	3.277 KiB	96.444032	3.2887	2439 bits/s	8163 bits/s

Here we see the traffic of Telnet 23 , FTP 21, DNS 53, HTTP 80. That's going from host 3 to host 2.

Lets look at the Endpoints which show all the IPs:

Wireshark · Endpoints · dns-remoteshell.pcap

Endpoint Settings

Name resolution

Limit to display filter

Copy

Map

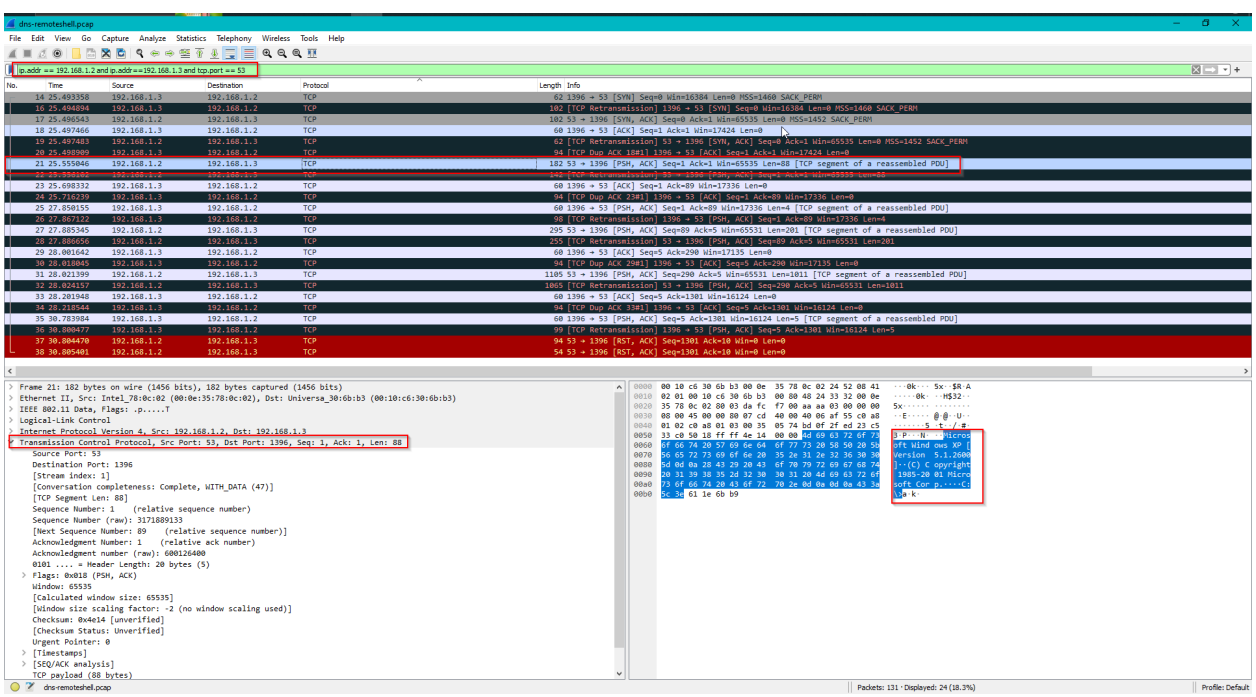
Ethernet · 5 | IPv4 · 6 | IPv6 | TCP · 16 | UDP · 4

Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
83.170.75.178	80	10	4.481 KiB	5	3.628 KiB	5	874 bytes
140.112.253.189	22604	1	96 bytes	0	0 bytes	1	96 bytes
192.168.1.2	21	24	1.828 KiB	12	888 bytes	12	984 bytes
192.168.1.2	23	33	5.267 KiB	15	3.887 KiB	18	1.380 KiB
192.168.1.2	53	24	4.349 KiB	10	3.277 KiB	14	1.071 KiB
192.168.1.2	80	23	4.257 KiB	10	3.277 KiB	13	1,003 bytes
192.168.1.2	1026	1	96 bytes	1	96 bytes	0	0 bytes
192.168.1.2	1108	5	3.311 KiB	2	188 bytes	3	3.127 KiB
192.168.1.2	1109	3	1.142 KiB	2	929 bytes	1	240 bytes
192.168.1.2	1110	5	1.171 KiB	3	686 bytes	2	513 bytes
192.168.1.3	1396	24	4.349 KiB	14	1.071 KiB	10	3.277 KiB
192.168.1.3	1399	12	936 bytes	6	492 bytes	6	444 bytes
192.168.1.3	1402	12	936 bytes	6	492 bytes	6	444 bytes
192.168.1.3	1403	33	5.267 KiB	18	1.380 KiB	15	3.887 KiB
192.168.1.3	1404	23	4.257 KiB	13	1,003 bytes	10	3.277 KiB
205.227.136.203	443	3	1.142 KiB	1	240 bytes	2	929 bytes

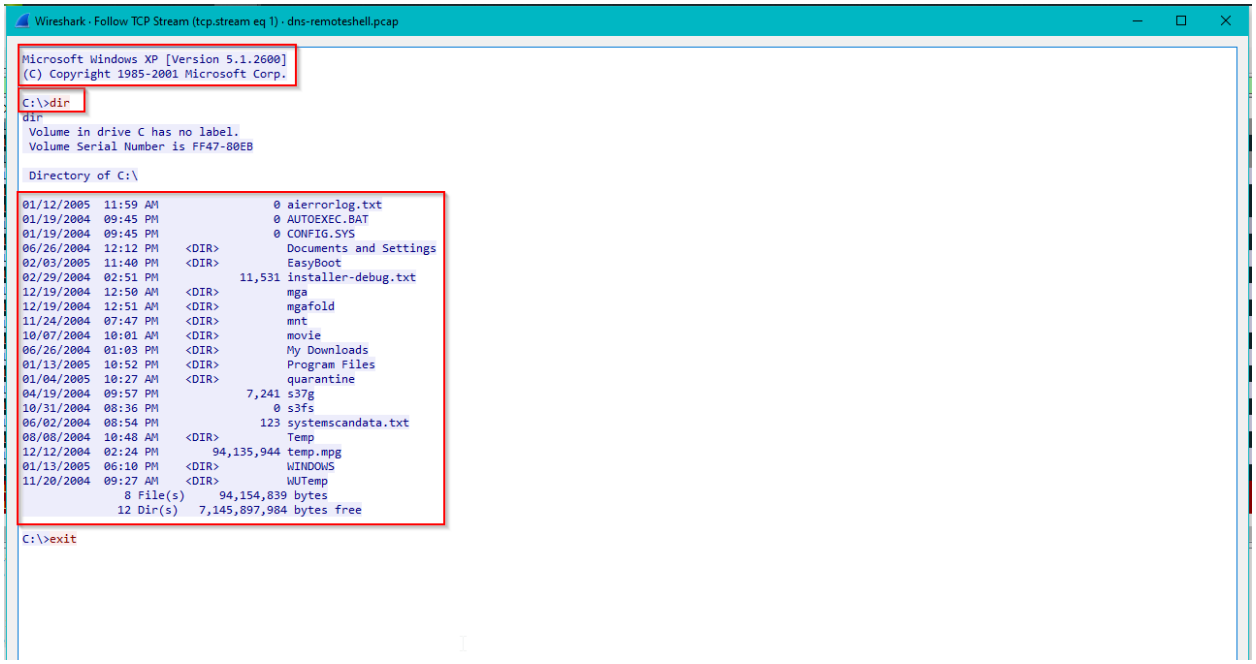
Here we see the port 53 again, so far we know that we are hunting for port 53 TCP:

Lets go to the Wireshark and filter for port 53 TCP:

After keep looking after the filter we found in the packet the Prompt of the CMD:

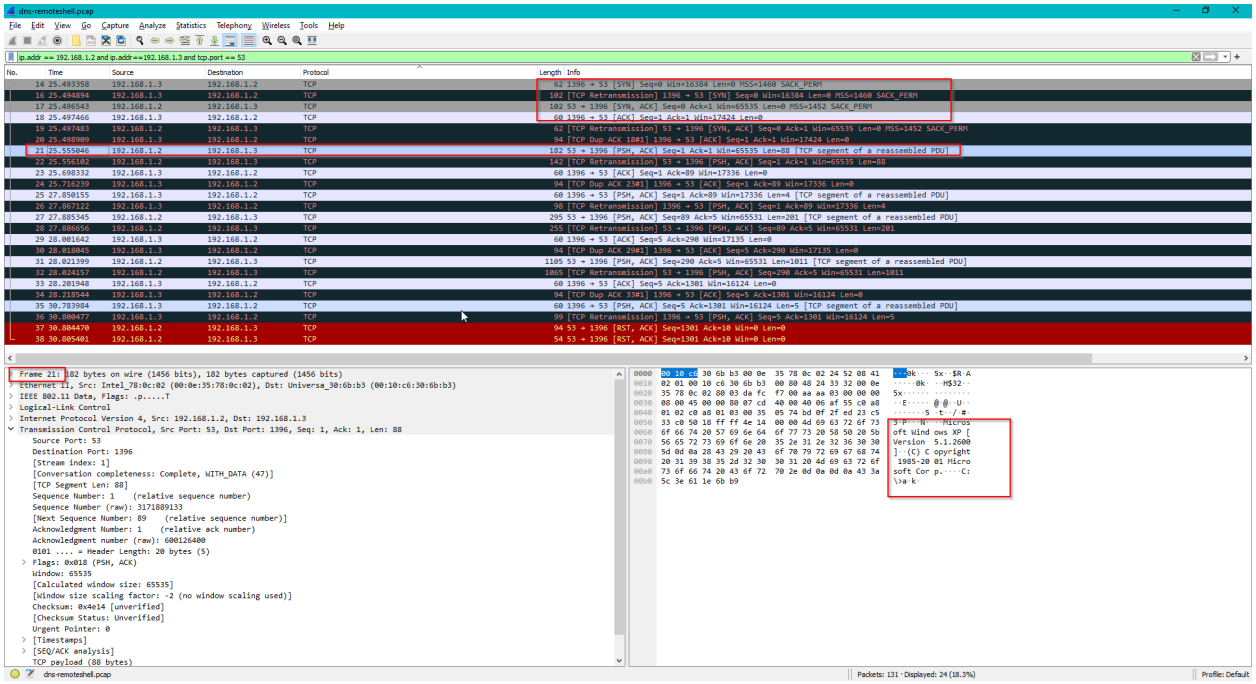


Lets follow its TCP stream by right clicking and then click Follow TCP stream:



Here we see the dir command is send to list the directory items and in response the attacker got the result of the command:

So the host 192.168.1.1 is hacked by the 3rd host 192.168.1.3 which it got shell, mean when the malware is executed on the host 1, it sent the prompt to the host 3.



Here we see first we see the 3 way handshake between the hosts and then the victim hosts 192.168.2.2 sends the command prompt to the attacker host 192.168.1.3 over port 53 TCP to cover or to show that it's a legit a traffic as the port 53 is open the host 192.168.1.2, buts its open for DNS which uses UDP but here its TCP.

Keep in mind that we focused on what we wanted to hunt for and it was TCP traffic over 53 port which is for UDP traffic:

One thing that we didn't answer was that we saw that host 3 also sent 3 UDP packet to the host 1 and it received even though it didn't have port 53 open: