

ITS Rossellini

26 novembre 2024

# **Esercizio Network**

## ***Simulazione d'Esame***

Dato il file denominato "**captureClient.pcapng**", analizzarlo e rispondere ai seguenti quesiti:

- 1) Quante conversazioni IPv4 sono presenti nella cattura del traffico fornita?
- 2) Dal pcap fornito si evidenzia la presenza di un server DHCP nella rete? Se sì, che indirizzo IPv4 ha?
- 3) Quante richieste DHCP sono presenti, quali sono gli IP che fanno la richiesta DHCP e quali sono i "Transaction ID"?
- 4) Qual è il server DNS presente nel file pcap fornito?
- 5) Quanti pacchetti etichettati come traffico DNS sono presenti nel pcap esaminato?

- 6) Trova l'indirizzo IPv4 associato al dominio "dns.msftncsi.com"
- 7) Qual è l'indirizzo IPv4 dell'host con cui il client avente IPv4 192.168.81.132 scambia il maggior volume di traffico di Bytes?
- 8) È presente traffico di tipo RDP?
- 9) Qual è l'indirizzo IPv4 del server C&C e da quale elemento puoi dedurlo?

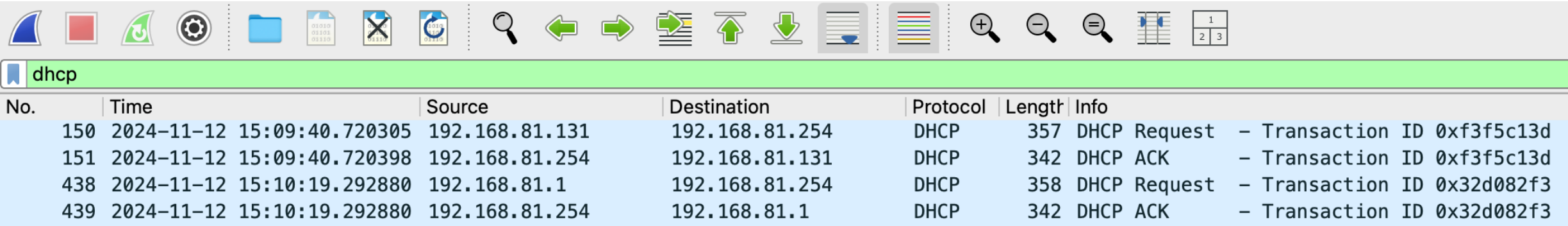
1) Quanti sessioni IPv4 sono presenti nella cattura del traffico fornita?

Nel Pcap fornito sono presenti 18 conversazioni IPv4 (*Pannello Conversation – tab IPv4*)

Wireshark · Conversations · captureClient.pcapng					
		Ethernet · 34		IPv4 · 18	IPv6 · 15
Address A	Address B	Packets	Bytes	Stream ID	
192.168.81.1	192.168.81.254	2	700 bytes	7	
192.168.81.1	224.0.0.22	5	300 bytes	8	
192.168.81.1	224.0.0.251	65	5 kB	9	
192.168.81.1	224.0.0.252	21	1 kB	10	
192.168.81.131	192.168.81.2	2	239 bytes	6	
192.168.81.131	192.168.81.132	2.334	188 kB	0	
192.168.81.131	192.168.81.254	2	699 bytes	2	
192.168.81.131	224.0.0.22	5	270 bytes	3	
192.168.81.131	224.0.0.252	1	75 bytes	4	
192.168.81.131	239.255.255.250	12	3 kB	13	
192.168.81.132	192.168.81.2	6	660 bytes	14	
192.168.81.132	192.168.81.133	7.855	4 MB	12	
192.168.81.132	192.168.81.255	2	220 bytes	15	
192.168.81.132	239.255.255.250	16	3 kB	1	
192.168.81.133	192.168.81.2	25	2 kB	11	
192.168.81.133	192.168.81.131	1	134 bytes	5	
192.168.81.133	192.168.81.255	9	1 kB	17	
192.168.81.133	224.0.0.252	4	256 bytes	16	

2) Dal pcap fornito si evidenzia la presenza di un server DHCP nella rete? Se sì, che indirizzo IPv4 ha?

Applicando il filtro "dhcp", posso individuare il traffico DHCP e posso vedere che le query sono rivolte tutte al server DHCP avente IPv4 192.168.81.254.



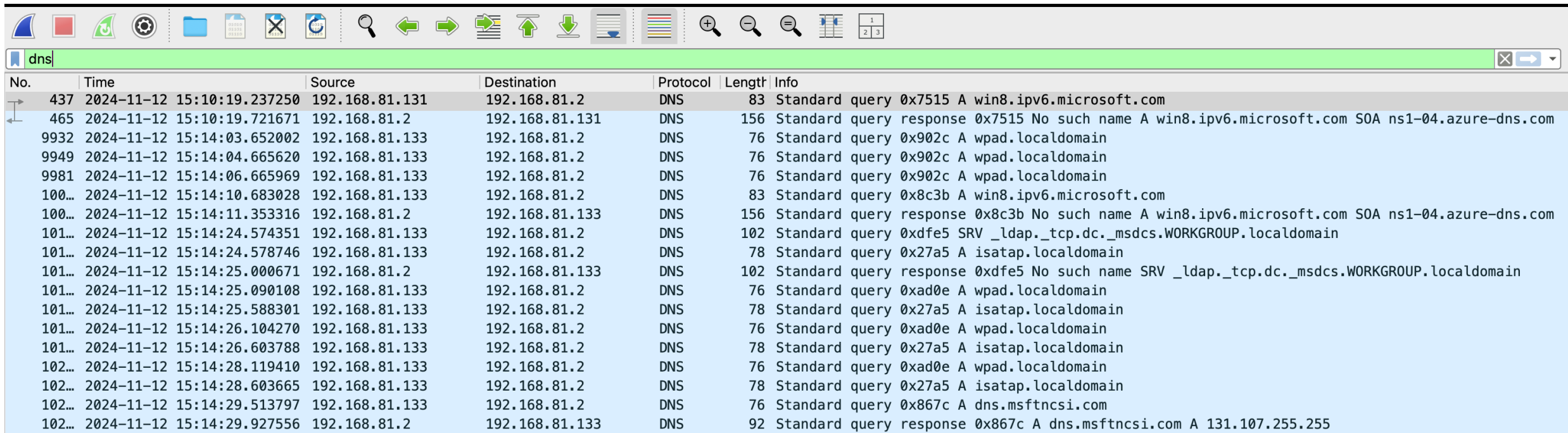
No.	Time	Source	Destination	Protocol	Length	Info
150	2024-11-12 15:09:40.720305	192.168.81.131	192.168.81.254	DHCP	357	DHCP Request - Transaction ID 0xf3f5c13d
151	2024-11-12 15:09:40.720398	192.168.81.254	192.168.81.131	DHCP	342	DHCP ACK - Transaction ID 0xf3f5c13d
438	2024-11-12 15:10:19.292880	192.168.81.1	192.168.81.254	DHCP	358	DHCP Request - Transaction ID 0x32d082f3
439	2024-11-12 15:10:19.292880	192.168.81.254	192.168.81.1	DHCP	342	DHCP ACK - Transaction ID 0x32d082f3

3) Quante richieste DHCP sono presenti, quali sono gli IPv4 che fanno la richiesta DHCP e quali sono i "Transaction ID"?

Mediante lo stesso filtro posso individuare che le richieste DHCP sono solo 2 e i relativi "Transaction ID" sono "0xf3f5c13d" e "0x32d082f3".

#### 4) Qual è il server DNS presente nel file pcap fornito?

Cambiando il filtro applicato con "dns" posso visualizzare query e response DNS e posso facilmente individuare che il server DNS è attestato sull'IPv4 192.168.81.2.



No.	Time	Source	Destination	Protocol	Length	Info
437	2024-11-12 15:10:19.237250	192.168.81.131	192.168.81.2	DNS	83	Standard query 0x7515 A win8.ipv6.microsoft.com
465	2024-11-12 15:10:19.721671	192.168.81.2	192.168.81.131	DNS	156	Standard query response 0x7515 No such name A win8.ipv6.microsoft.com SOA ns1-04.azure-dns.com
9932	2024-11-12 15:14:03.652002	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
9949	2024-11-12 15:14:04.665620	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
9981	2024-11-12 15:14:06.665969	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
100...	2024-11-12 15:14:10.683028	192.168.81.133	192.168.81.2	DNS	83	Standard query 0x8c3b A win8.ipv6.microsoft.com
100...	2024-11-12 15:14:11.353316	192.168.81.2	192.168.81.133	DNS	156	Standard query response 0x8c3b No such name A win8.ipv6.microsoft.com SOA ns1-04.azure-dns.com
101...	2024-11-12 15:14:24.574351	192.168.81.133	192.168.81.2	DNS	102	Standard query 0xdfe5 SRV _ldap._tcp.dc._msdcs.WORKGROUP.localdomain
101...	2024-11-12 15:14:24.578746	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
101...	2024-11-12 15:14:25.000671	192.168.81.2	192.168.81.133	DNS	102	Standard query response 0xdfe5 No such name SRV _ldap._tcp.dc._msdcs.WORKGROUP.localdomain
101...	2024-11-12 15:14:25.090108	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
101...	2024-11-12 15:14:25.588301	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
101...	2024-11-12 15:14:26.104270	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
101...	2024-11-12 15:14:26.603788	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
102...	2024-11-12 15:14:28.119410	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
102...	2024-11-12 15:14:28.603665	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
102...	2024-11-12 15:14:29.513797	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x867c A dns.msftncsi.com
102...	2024-11-12 15:14:29.927556	192.168.81.2	192.168.81.133	DNS	92	Standard query response 0x867c A dns.msftncsi.com A 131.107.255.255

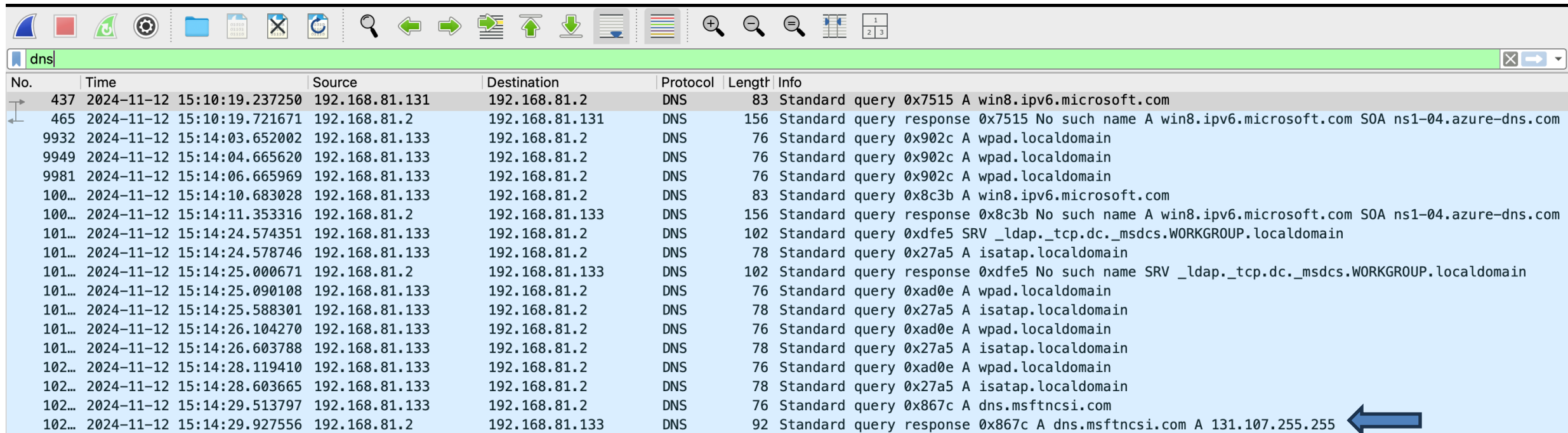
5) Quanti pacchetti etichettati come traffico DNS sono presenti nel pcap esaminato?

Quanti pacchetti etichettati come traffico DNS sono presenti nel pcap esaminato?  
Posso andare a vedere, all'interno del Tab "Statistics" → "Protocol Hierarchy" che sono presenti 18 pacchetti DNS

Wireshark · Protocol Hierarchy Statistics · captureClient.pcapng							
Protocol	▼	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets
▼ Frame		100.0	18	100.0	1618	51	0
▼ Ethernet		100.0	18	15.6	252	8	0
▼ Internet Protocol Version 4		100.0	18	22.2	360	11	0
▼ User Datagram Protocol		100.0	18	8.9	144	4	0
Domain Name System		100.0	18	53.3	862	27	18

## 6) Trova l'indirizzo IPv4 associato al dominio "dns.msftncsi.com"

Nell'output del filtro "dns" è possibile identificare che la response alla query DNS per il dominio "dns.msftncsi.com", riporta l'indirizzo IPv4 131.107.255.255



No.	Time	Source	Destination	Protocol	Length	Info
437	2024-11-12 15:10:19.237250	192.168.81.131	192.168.81.2	DNS	83	Standard query 0x7515 A win8.ipv6.microsoft.com
465	2024-11-12 15:10:19.721671	192.168.81.2	192.168.81.131	DNS	156	Standard query response 0x7515 No such name A win8.ipv6.microsoft.com SOA ns1-04.azure-dns.com
9932	2024-11-12 15:14:03.652002	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
9949	2024-11-12 15:14:04.665620	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
9981	2024-11-12 15:14:06.665969	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x902c A wpad.localdomain
100...	2024-11-12 15:14:10.683028	192.168.81.133	192.168.81.2	DNS	83	Standard query 0x8c3b A win8.ipv6.microsoft.com
100...	2024-11-12 15:14:11.353316	192.168.81.2	192.168.81.133	DNS	156	Standard query response 0x8c3b No such name A win8.ipv6.microsoft.com SOA ns1-04.azure-dns.com
101...	2024-11-12 15:14:24.574351	192.168.81.133	192.168.81.2	DNS	102	Standard query 0xdfe5 SRV _ldap._tcp.dc._msdcs.WORKGROUP.localdomain
101...	2024-11-12 15:14:24.578746	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
101...	2024-11-12 15:14:25.000671	192.168.81.2	192.168.81.133	DNS	102	Standard query response 0xdfe5 No such name SRV _ldap._tcp.dc._msdcs.WORKGROUP.localdomain
101...	2024-11-12 15:14:25.090108	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
101...	2024-11-12 15:14:25.588301	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
101...	2024-11-12 15:14:26.104270	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
101...	2024-11-12 15:14:26.603788	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
102...	2024-11-12 15:14:28.119410	192.168.81.133	192.168.81.2	DNS	76	Standard query 0xad0e A wpad.localdomain
102...	2024-11-12 15:14:28.603665	192.168.81.133	192.168.81.2	DNS	78	Standard query 0x27a5 A isatap.localdomain
102...	2024-11-12 15:14:29.513797	192.168.81.133	192.168.81.2	DNS	76	Standard query 0x867c A dns.msftncsi.com
102...	2024-11-12 15:14:29.927556	192.168.81.2	192.168.81.133	DNS	92	Standard query response 0x867c A dns.msftncsi.com A 131.107.255.255

Standard query response 0x867c A dns.msftncsi.com A 131.107.255.255



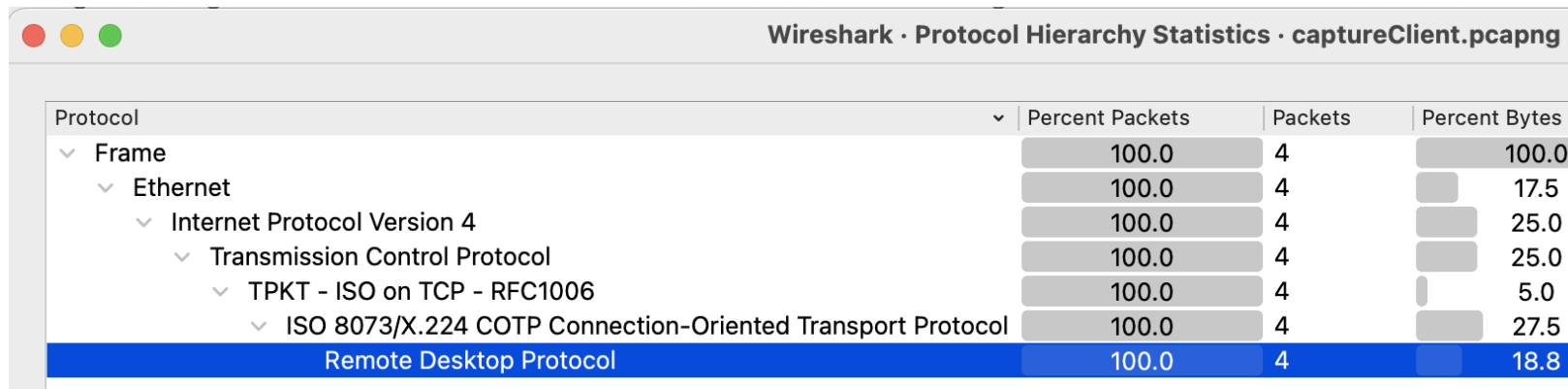
7) Qual è l'indirizzo IPv4 dell'host con cui il client avente IPv4 192.168.81.132 scambia il maggior volume di traffico di Bytes?

Dal Tab "Statistics" → "Conversations" clicchiamo sul Tab "IPv4", ordiniamo per la colonna "Bytes" e possiamo identificare che l'host con cui viene scambiato più traffico è il 192.168.81.133.

Wireshark · Conversations · captureClient.pcapng				
Ethernet · 34 IPv4 · 18 IPv6 · 15				
Address A	Address B	Packets	Bytes ▾	Stream ID
192.168.81.132	192.168.81.133	7.855	4 MB	12
192.168.81.131	192.168.81.132	2.334	188 kB	0
192.168.81.1	224.0.0.251	65	5 kB	9
192.168.81.132	239.255.255.250	16	3 kB	1
192.168.81.131	239.255.255.250	12	3 kB	13
192.168.81.132	192.168.81.133	25	2 MB	11

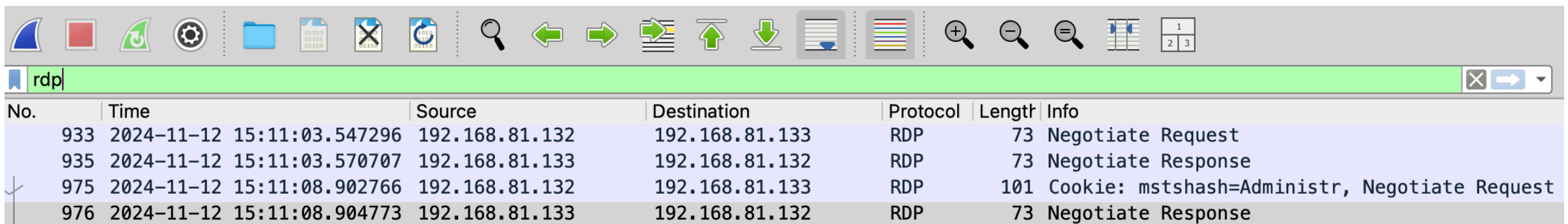
8) È presente traffico di tipo RDP?

Sì, è presente traffico RDP e lo posso vedere sia dal Tab "Protocol Hierarchy" sia semplicemente impostando il filtro "rdp".



Wireshark - Protocol Hierarchy Statistics - captureClient.pcapng

Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	4	100.0
Ethernet	100.0	4	17.5
Internet Protocol Version 4	100.0	4	25.0
Transmission Control Protocol	100.0	4	25.0
TPKT - ISO on TCP - RFC1006	100.0	4	5.0
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol	100.0	4	27.5
Remote Desktop Protocol	100.0	4	18.8



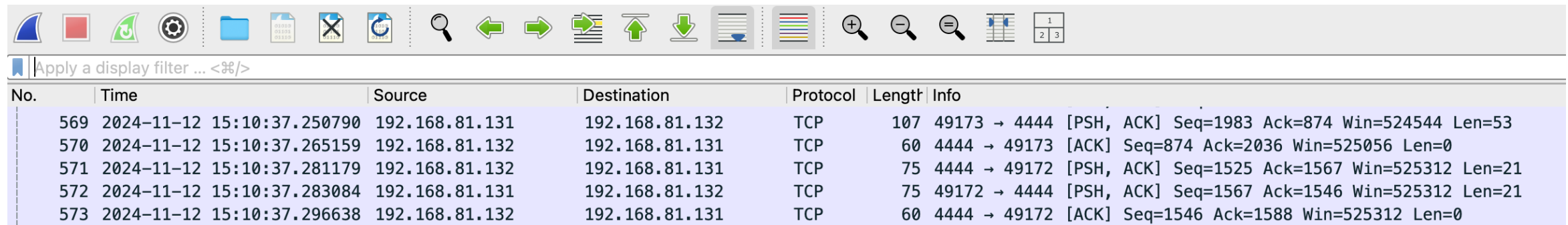
rdp

No.	Time	Source	Destination	Protocol	Length	Info
933	2024-11-12 15:11:03.547296	192.168.81.132	192.168.81.133	RDP	73	Negotiate Request
935	2024-11-12 15:11:03.570707	192.168.81.133	192.168.81.132	RDP	73	Negotiate Response
975	2024-11-12 15:11:08.902766	192.168.81.132	192.168.81.133	RDP	101	Cookie: msthash=Administr, Negotiate Request
976	2024-11-12 15:11:08.904773	192.168.81.133	192.168.81.132	RDP	73	Negotiate Response

9) Qual'è l'indirizzo IPv4 del server C&C e da quale elemento puoi dedurlo?

Anche solo scorrendo la lista dei pacchetti, posso identificare una notevole quantità di traffico scambiato tra porte random dell'host 192.168.81.131 verso la porta TCP 4444 dell'IP 192.168.81.132.

Come abbiamo visto durante il corso, tale porta è quella impostata di default quando vengono create backdoor, malware, ecc...



Apply a display filter ... <%%/>

No.	Time	Source	Destination	Protocol	Length	Info
569	2024-11-12 15:10:37.250790	192.168.81.131	192.168.81.132	TCP	107	49173 → 4444 [PSH, ACK] Seq=1983 Ack=874 Win=524544 Len=53
570	2024-11-12 15:10:37.265159	192.168.81.132	192.168.81.131	TCP	60	4444 → 49173 [ACK] Seq=874 Ack=2036 Win=525056 Len=0
571	2024-11-12 15:10:37.281179	192.168.81.132	192.168.81.131	TCP	75	4444 → 49172 [PSH, ACK] Seq=1525 Ack=1567 Win=525312 Len=21
572	2024-11-12 15:10:37.283084	192.168.81.131	192.168.81.132	TCP	75	49172 → 4444 [PSH, ACK] Seq=1567 Ack=1546 Win=525312 Len=21
573	2024-11-12 15:10:37.296638	192.168.81.132	192.168.81.131	TCP	60	4444 → 49172 [ACK] Seq=1546 Ack=1588 Win=525312 Len=0



**KEEP  
CALM**

**AND**

**IN BOCCA AL LUPO RAGAZZI!**