hacktheblue,pcap(wireshark)

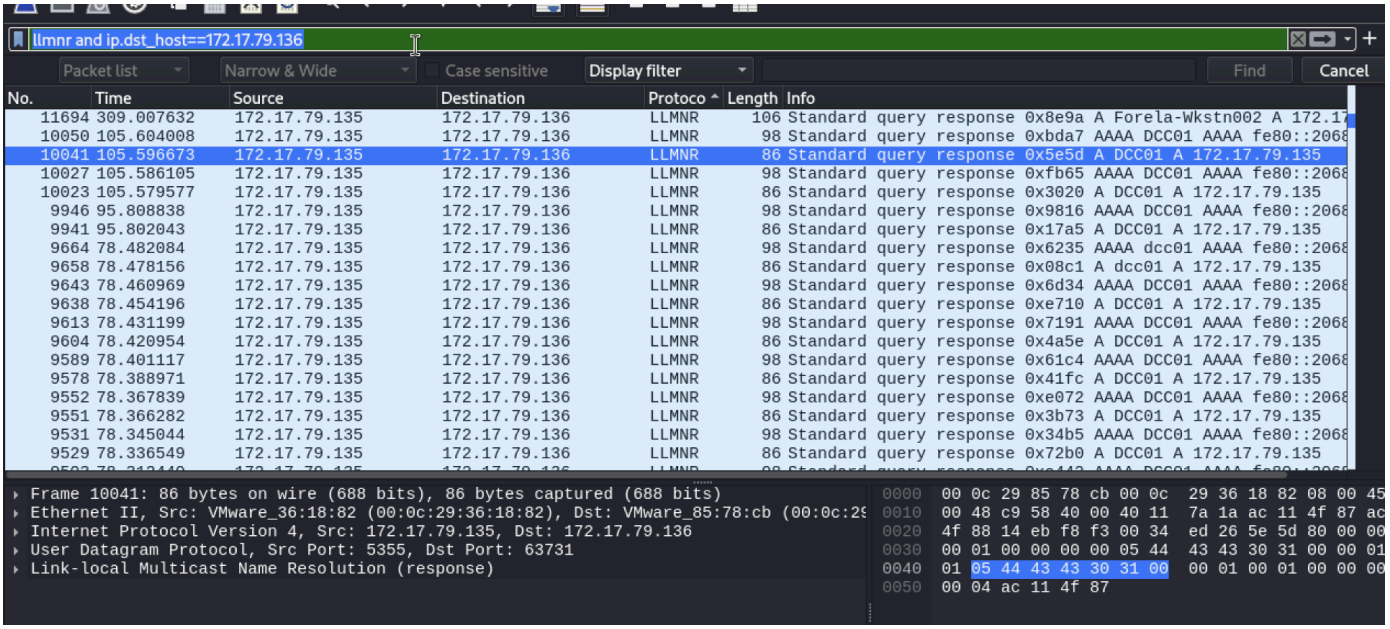
```
Sherlock Scenario

The IDS device alerted us to a possible rogue device in the internal Active Directory network. The Intrusion Detection System also indicated signs of LLMNR traffic, which is unusual. It is suspected that an LLMNR poisoning attack occurred. The LLMNR traffic was directed towards Forela-WKstn002, which has the IP address 172.17.79.136. A limited packet capture from the surrounding time is provided to you, our Network Forensics expert. Since this occurred in the Active Directory VLAN, it is suggested that we perform network threat hunting with the Active Directory attack vector in mind, specifically focusing on LLMNR poisoning.
* * *
About Noxious

In this sherlock, players will go through network traffic and uncover credential-stealing technique by abusing the LLMNR protocol feature in Windows. Players will learn how a victim made a typo navigating to a network share and how the attacker was using the Responder tool to steal hashes and pose as a legitimate device in the internal network. Players will also learn to crack NTLMV2 hashes by gathering information from SMB traffic.
```

文件：capture.pcap
使用工具：wirshark

Task 1

Its suspected by the security team that there was a rogue device in Forela's internal network running responder tool to perform an LLMNR Poisoning attack. Please find the malicious IP Address of the machine.

filter : `llmnr and ip.dst_host==172.17.79.136`

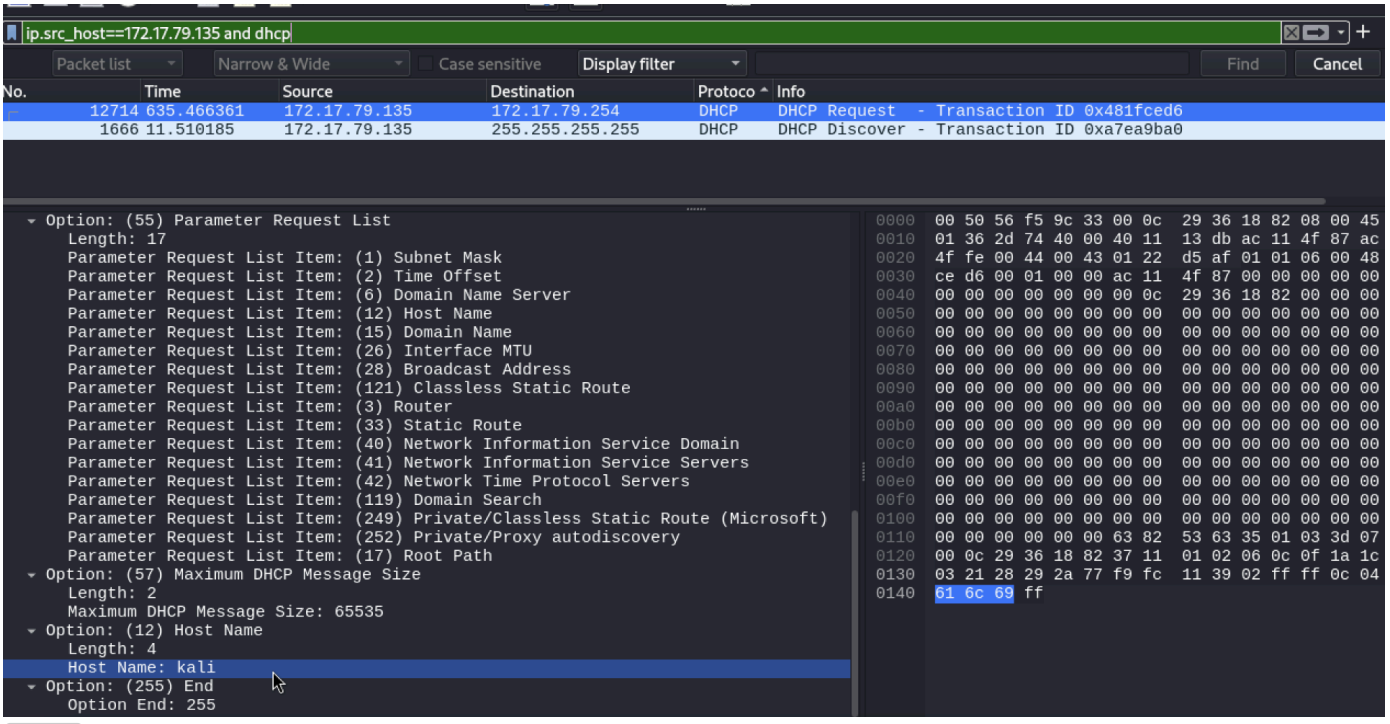


`172.17.79.135`

Task 2

What is the hostname of the rogue machine?

filter : `ip.src_host==172.17.79.135 and dhcp`

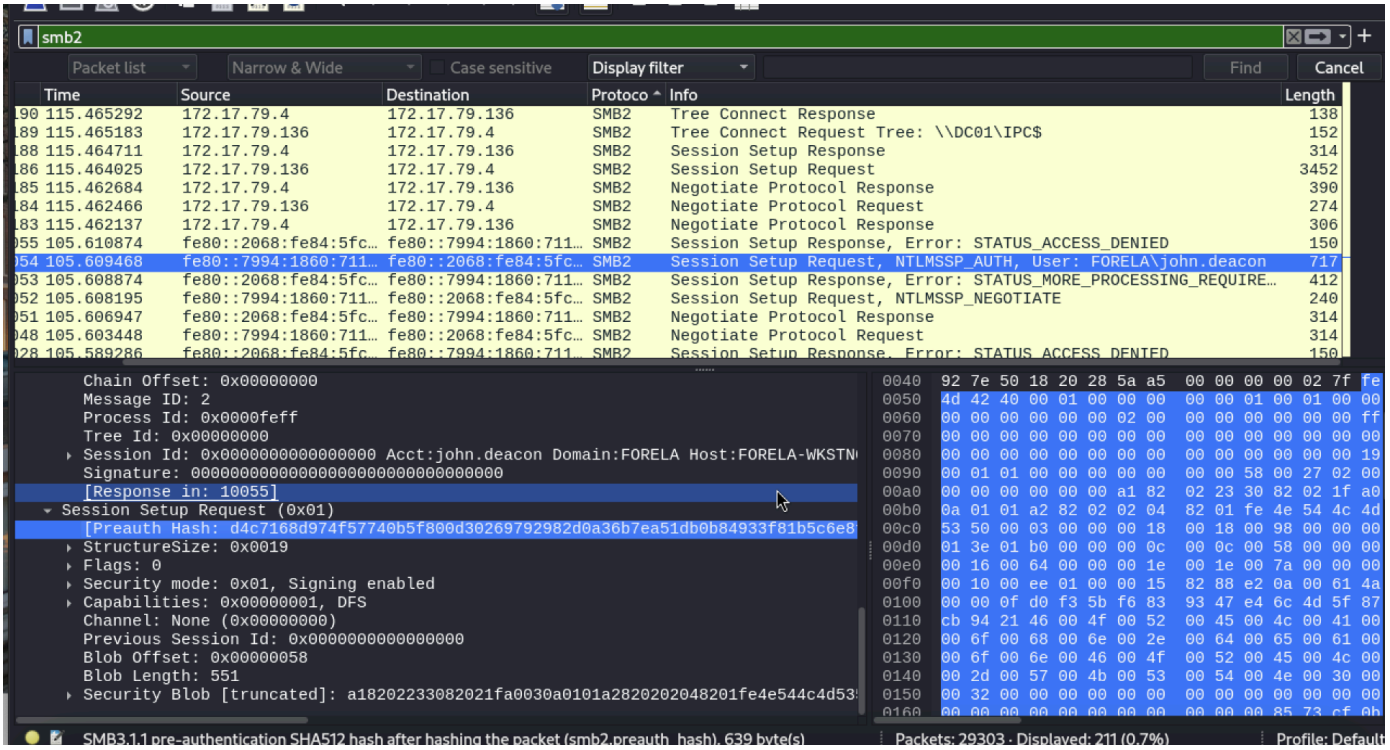


`kali`

Task 3

Now we need to confirm whether the attacker captured the user's hash and it is crackable!! What is the username whose hash was captured?

filter：`smb2`

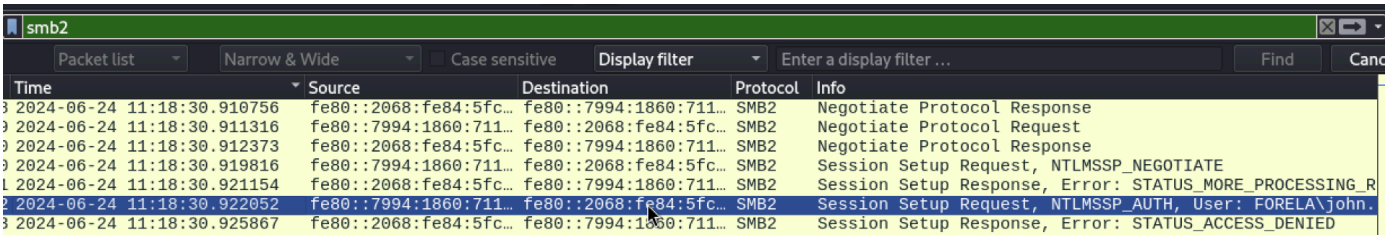


`john.deacon`

Task 4

In NTLM traffic we can see that the victim credentials were relayed multiple times to the attacker's machine. When were the hashes captured the First time?

同上，只是選最早時間

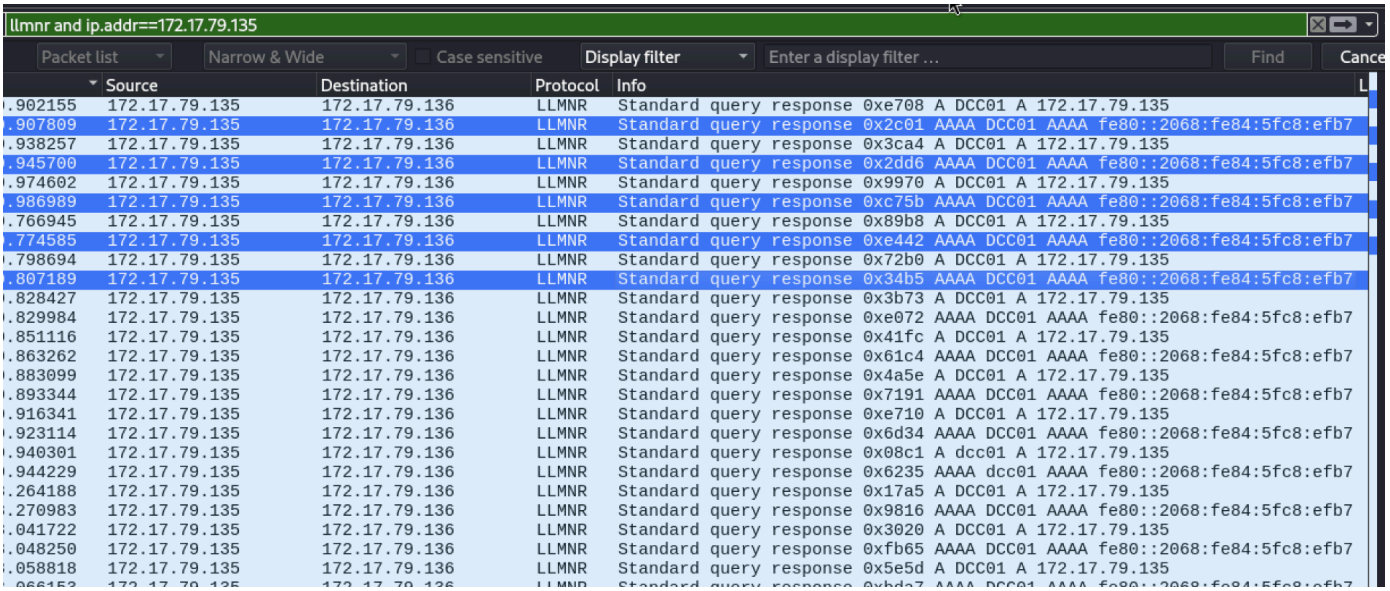


`2024-06-24 11:18:30`

Task 5

What was the typo made by the victim when navigating to the file share that caused his credentials to be leaked?

filter：`llmnr and ip.addr==172.17.79.135`

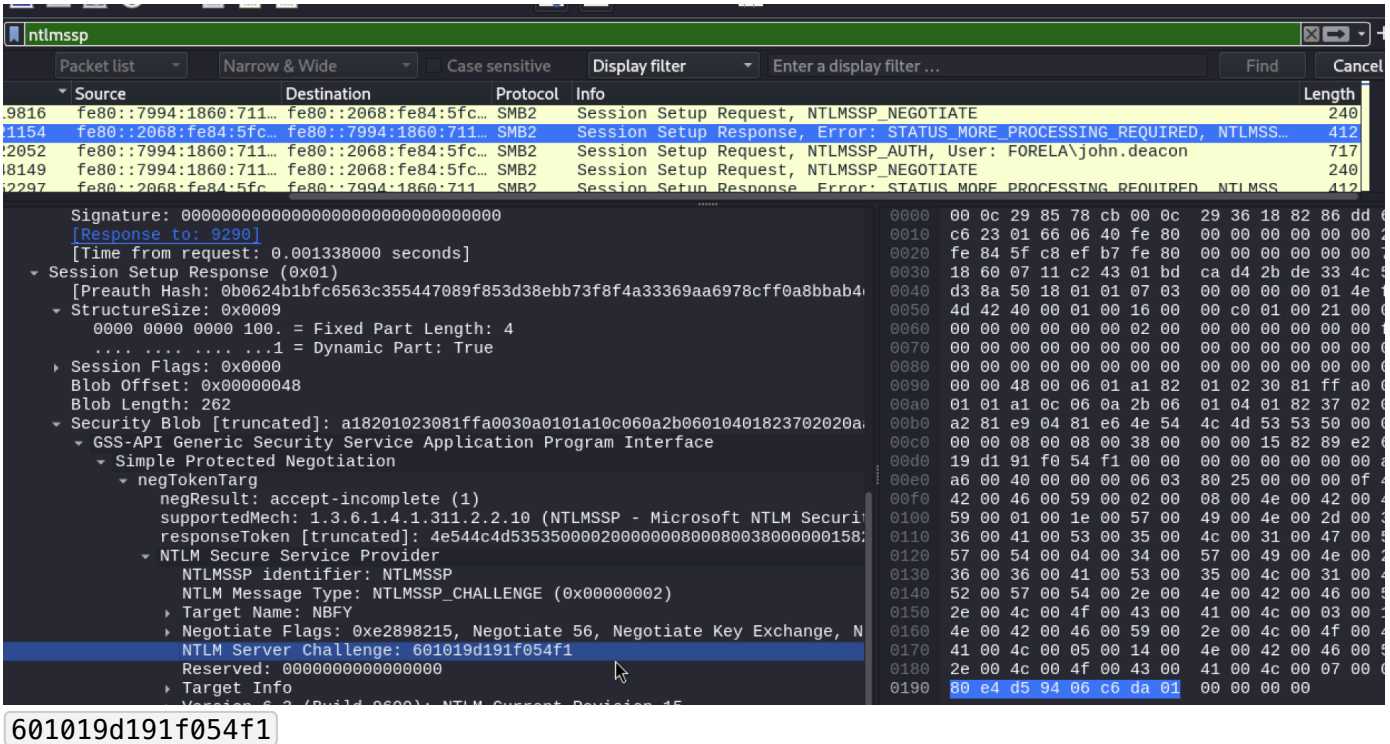


`DCC01`

Task 6

To get the actual credentials of the victim user we need to stitch together multiple values from the ntlm negotiation packets. What is the NTLM server challenge value?

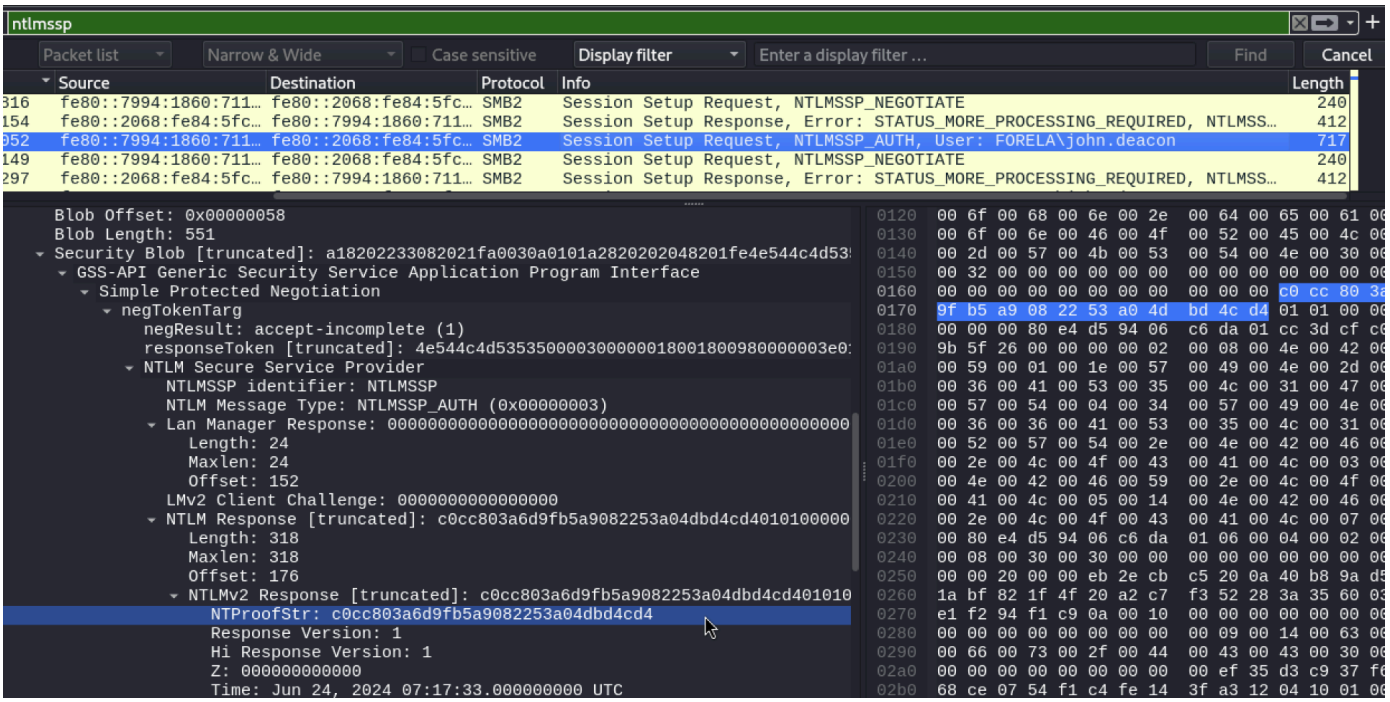
filter：`ntlmssp`



`601019d191f054f1`

Task 7

Now doing something similar find the NTProofStr value.



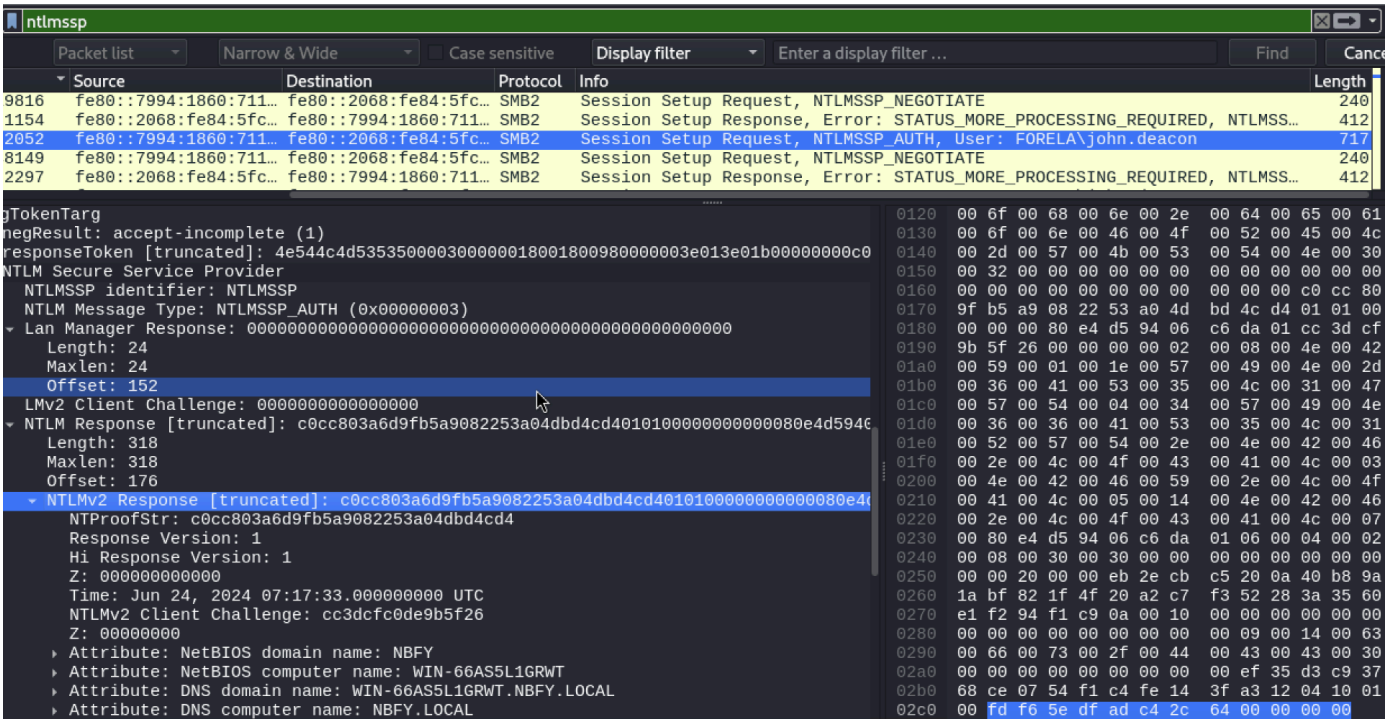
`c0cc803a6d9fb5a9082253a04dbd4cd4`

Task 8

To test the password complexity, try recovering the password from the information found from packet capture. This is a crucial step as this way we can find whether the attacker was able to crack this and how quickly.

重點條件：User::Domain:ServerChallenge:NTProofStr:NTLMv2Response

NTLMv2Response =>從值中刪除前32 個字元




```
john.deacon::FORELA:601019d191f054f1:c0cc803a6d9fb5a9082253a04dbd4cd4:010100
00000000000080e4d59406c6da01cc3dcfc0de9b5f2600000000020008004e0042004600590001
001e00570049004e002d00360036004100530035004c00310047005200570054000400340057
```

```
0049004e002d00360036004100530035004c00310047005200570054002e004e004200460059
002e004c004f00430041004c00030014004e004200460059002e004c004f00430041004c0005
0014004e004200460059002e004c004f00430041004c00700080080e4d59406c6da01060004
0002000000080030003000000000000000000000000200000eb2ecbc5200a40b89ad5831abf
821f4f20a2c7f352283a35600377e1f294f1c90a0010000000000000000000000000000000000
0009001400630069006600730002f00440043004300300031000000000000000000
```

* * *

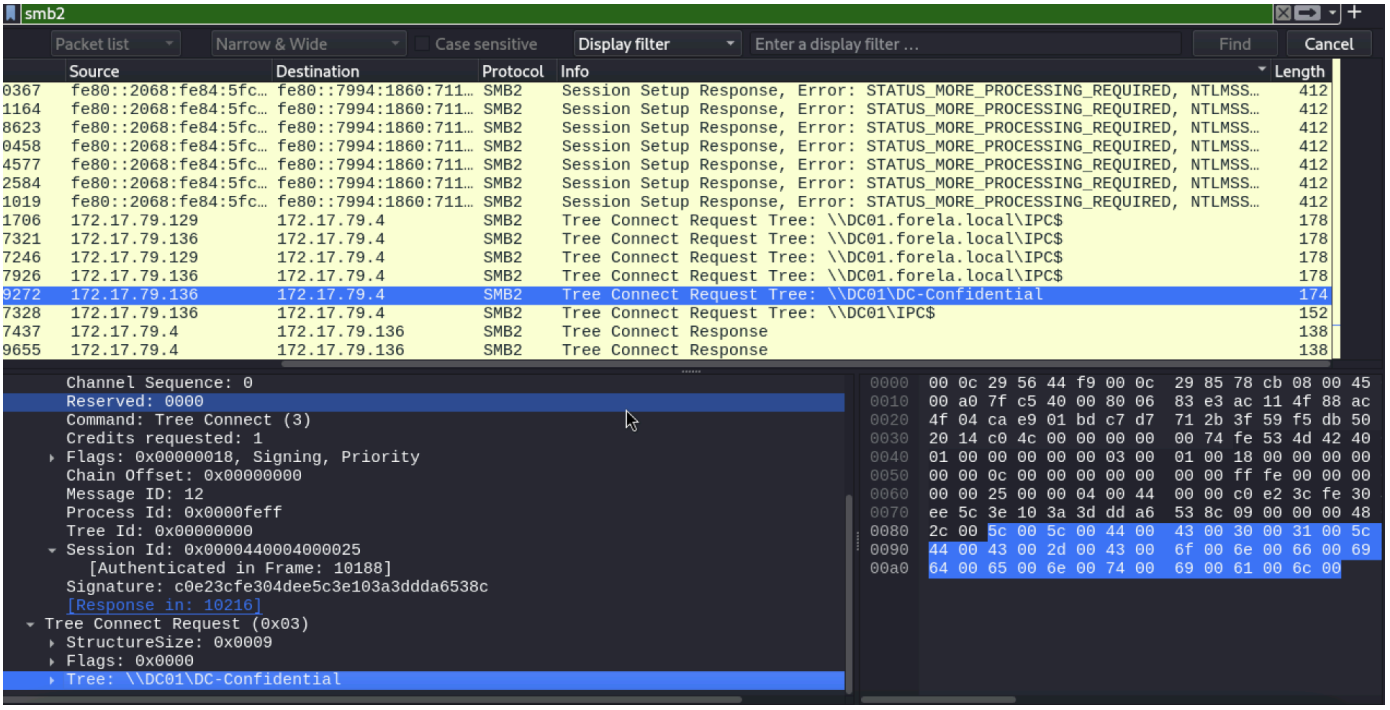
解碼：`hashcat -a 0 -m 5600 hash.txt /usr/share/wordlists/rockyou.txt --potfile-disable --force`

`NotMyPassword0k?`

Task 9

Just to get more context surrounding the incident, what is the actual file share that the victim was trying to navigate to?

filter：`SMB2`



`\\DC01\DC-Confidential`