Network Forensic Analysis: LLMNR/NBT-NS Poisoning & Credential Access

Analyst: Mduduzi William Radebe

Date: 07 February 2026

Platform: CyberDefenders

Lab: PoisonedCredentials

Case ID: 2026-PC-009

1. Executive Summary

A forensic investigation was conducted on a network traffic capture (PCAP) to identify an suspected **Man-in-the-Middle (MitM)** attack. The analysis confirmed that a rogue machine utilized **LLMNR (Link-Local Multicast Name Resolution)** poisoning to intercept requests intended for a legitimate file share. This resulted in the successful compromise of a user's NTLM credentials and unauthorized access to an internal accounting system via the **SMB** protocol.

2. Project Objective

The primary goal was to dissect the network traffic to:

- Identify the origin of the malicious "poisoned" responses.
- Determine the specific queries that triggered the attack.
- Identify all affected (victim) machines.
- Extract the compromised username and identify the target host accessed by the adversary.

3. Tools & Methodology

The Analyst Toolkit

- **Wireshark:** Used for deep packet inspection and protocol analysis.
- **Filters:** Leveraged specific display filters to isolate malicious traffic from background noise.
- **TCP Stream Following:** Used to reconstruct the "conversation" between the attacker and victims.

The "Step-by-Step" Workflow

Phase 1: Identifying the Catalyst (The Mistyped Query)

Action: I filtered for LLMNR traffic originating from the suspected victim IP 192.168.232.162.

Filter: ip.addr == 192.168.232.162 && llmnr

Observation: The machine was broadcasting a query for the name **fileshaare**.

Analyst Note: The double 'a' in the name confirms a user typo. Because this name doesn't exist on the DNS server, the computer resorted to LLMNR, which "shouts" to the whole network for help.

Phase 2: Locating the Rogue Entity

Action: I utilized Wireshark's **Statistics > Endpoints** tool to find the most active IPv4 addresses, then looked for who responded to the fileshaare query.

Observation: Machine **192.168.232.215** immediately responded to the broadcast, claiming to be the location of the (non-existent) fileshaare.

Conclusion: 192.168.232.215 is confirmed as the **Rogue Machine** (Attacker).

Phase 3: Scope of Impact (The Second Victim)

Action: I filtered for all traffic where the Rogue Machine sent responses to different hosts.

Filter: ip.src == 192.168.232.215

Observation: I identified a second machine, **192.168.232.176**, receiving poisoned responses from the attacker. This confirms the attack was broad and automated (likely using a tool like **Responder**).

Phase 4: Credential Theft Analysis

Action: I focused on the **SMB (Server Message Block)** protocol to see if any login attempts were intercepted. I selected an SMB packet and used **Follow > TCP Stream**.

Observation: Within the NTLM authentication exchange (NTLMSSP), the attacker forced the victim to authenticate.

Findings: The compromised account was identified as **janesmith**.

Phase 5: Action on Objectives

Action: I tracked the attacker's activity after the credential theft to see what internal resource they targeted.

Filter: ip.addr == 192.168.232.215 && smb2

Observation: The attacker used the stolen credentials to connect to a new machine.

Target Hostname: AccountingPC.

4. Technical Findings Summary

Metric	Detail
Initial Mistyped Query	fileshaare
Rogue Machine IP	192.168.232.215
Victim IP #1	192.168.232.162
Victim IP #2	192.168.232.176
Compromised User	janesmith
Targeted Destination	AccountingPC

5. Analyst Reflections

Struggles & Challenges

- **Noise Filtering:** Initial analysis was difficult due to the sheer volume of background traffic. Learning to use ip.addr in combination with llmnr was the "lightbulb moment" that cleared the noise.
- **Understanding Streams:** Following a TCP stream can be overwhelming for a beginner. It took a few tries to find the specific "NTLMSSP" (login) part of the conversation among the thousands of bytes of data.

Lessons Learned

- **Protocol Dangers:** I learned that LLMNR and NBT-NS are dangerous legacy protocols that should be **disabled** via Group Policy in a secure environment.
- **The Power of Typo:** This lab taught me that a single misspelled word by a user can lead to an entire network being compromised if local name resolution is not secured.
- **SMB Signing:** I now understand that enforcing **SMB Signing** would prevent an attacker from easily relaying these stolen credentials to other machines like the AccountingPC.

6. Recommendations (SOC Strategy)

1. **Immediate Action:** Disable LLMNR and NBT-NS on all workstations and servers via GPO.
2. **Monitoring:** Configure SIEM alerts for any "LLMNR Response" packets originating from non-IT subnets.
3. **Credential Hygiene:** Reset the password for janesmith immediately and audit the AccountingPC for any unauthorized file access or persistence mechanisms.

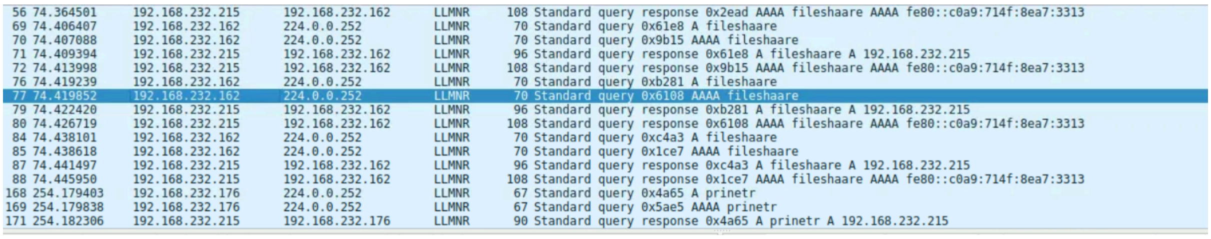
Analyst Signature

Mduduzi William Radebe

SOC Analyst in Training

Notes and Screenshots

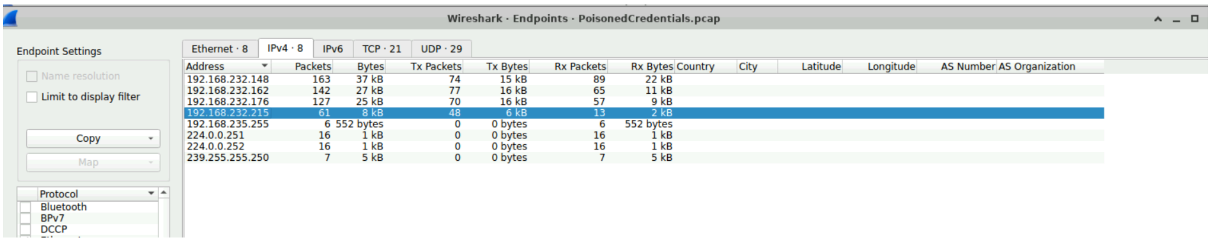
Q1:



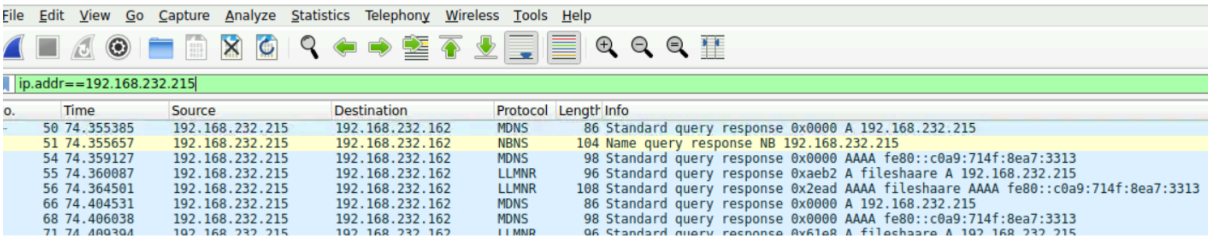
```
 56 74.364501   192.168.232.215   192.168.232.162   LLMNR   108 Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
 69 74.406407   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0x61e8 A fileshaare
 70 74.407088   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0x9b15 AAAA fileshaare
 71 74.409394   192.168.232.215   192.168.232.162   LLMNR    96 Standard query response 0x61e8 A fileshaare A 192.168.232.215
 72 74.413998   192.168.232.215   192.168.232.162   LLMNR   108 Standard query response 0x9b15 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
 76 74.419239   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0xb281 A fileshaare
 77 74.419852   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0x6108 AAAA fileshaare
 79 74.422420   192.168.232.215   192.168.232.162   LLMNR    96 Standard query response 0xb281 A fileshaare A 192.168.232.215
 80 74.426719   192.168.232.215   192.168.232.162   LLMNR   108 Standard query response 0x6108 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
 84 74.438101   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0xc4a3 A fileshaare
 85 74.438618   192.168.232.162   224.0.0.252       LLMNR    70 Standard query 0x1ce7 AAAA fileshaare
 87 74.441497   192.168.232.215   192.168.232.162   LLMNR    96 Standard query response 0xc4a3 A fileshaare A 192.168.232.215
 88 74.445950   192.168.232.215   192.168.232.162   LLMNR   108 Standard query response 0x1ce7 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
168 254.179403  192.168.232.176   224.0.0.252       LLMNR    67 Standard query 0x4a65 A prinetr
169 254.179838  192.168.232.176   224.0.0.252       LLMNR    67 Standard query 0x5ae5 AAAA prinetr
171 254.182306  192.168.232.215   192.168.232.176   LLMNR    90 Standard query response 0x4a65 A prinetr A 192.168.232.215
```

Q2:

Statistics > Endpoints >ipv4 add 192.168.232.215



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
192.168.232.148	163	37 kB	74	15 kB	89	22 kB						
192.168.232.162	142	27 kB	77	16 kB	65	11 kB						
192.168.232.176	127	25 kB	70	16 kB	57	9 kB						
192.168.232.215	61	8 kB	48	6 kB	13	2 kB						
192.168.235.255	6	552 bytes	0	0 bytes	6	552 bytes						
224.0.0.251	16	1 kB	0	0 bytes	16	1 kB						
224.0.0.252	16	1 kB	0	0 bytes	16	1 kB						
239.255.255.250	7	5 kB	0	0 bytes	7	5 kB						

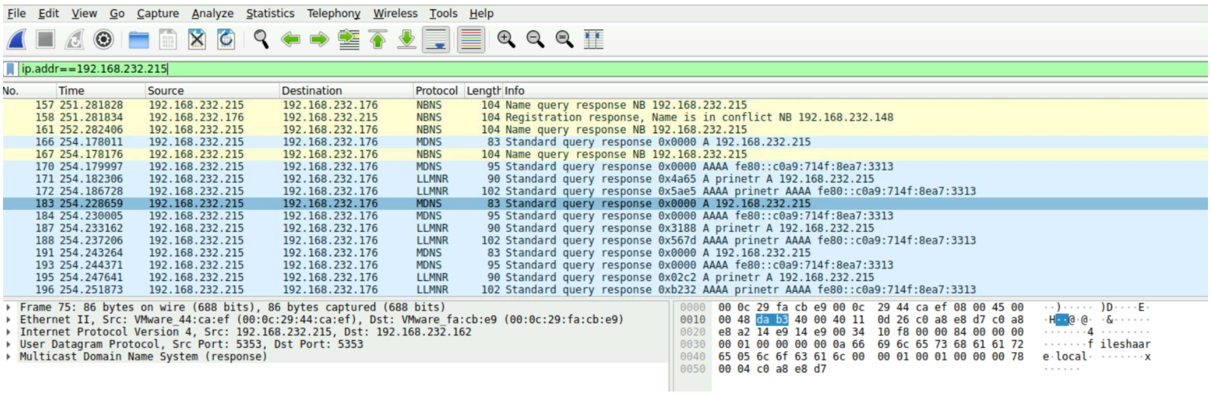


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.232.215

```
o.      Time        Source            Destination       Protocol Length Info
     50 74.355385   192.168.232.215   192.168.232.162   MDNS      86 Standard query response 0x0000 A 192.168.232.215
     51 74.355657   192.168.232.215   192.168.232.162   NBNS     104 Name query response NB 192.168.232.215
     54 74.359127   192.168.232.215   192.168.232.162   MDNS      98 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
     55 74.360087   192.168.232.215   192.168.232.162   LLMNR     96 Standard query response 0xaeb2 A fileshaare A 192.168.232.215
     56 74.364501   192.168.232.215   192.168.232.162   LLMNR    108 Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
     66 74.404531   192.168.232.215   192.168.232.162   MDNS      86 Standard query response 0x0000 A 192.168.232.215
     68 74.406038   192.168.232.215   192.168.232.162   MDNS      98 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
     71 74.409394   192.168.232.215   192.168.232.162   LLMNR     96 Standard query response 0x61e8 A fileshaare A 192.168.232.215
```

Q3



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==192.168.232.215

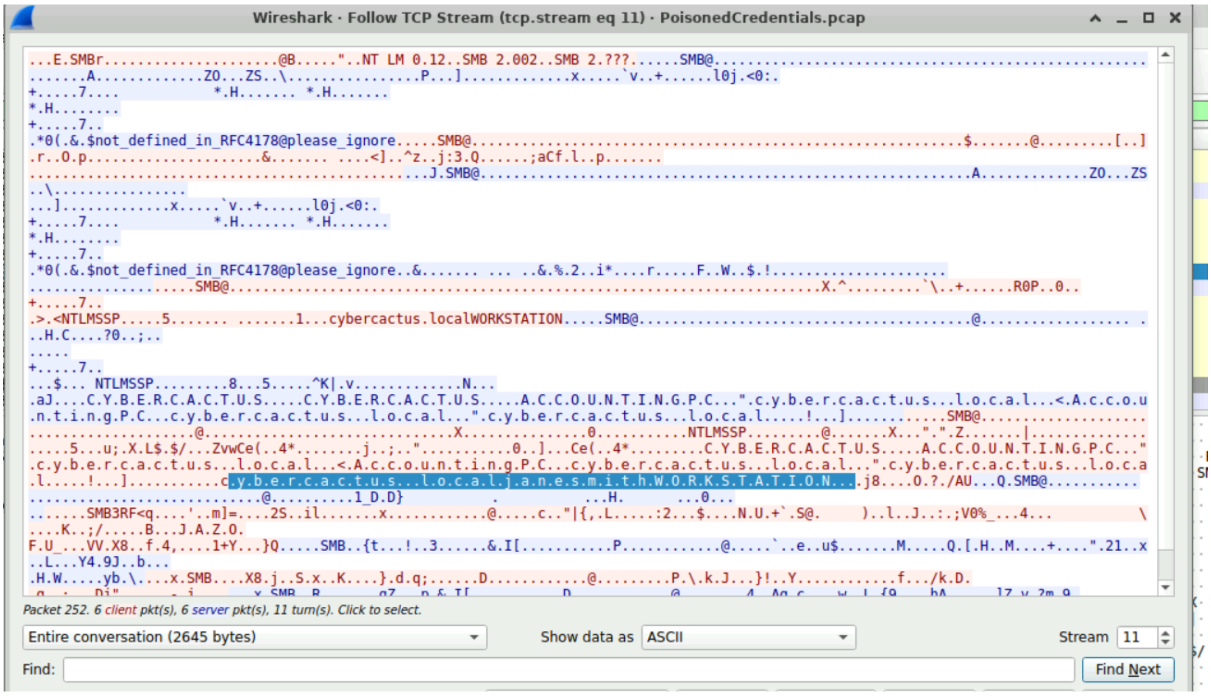
```
No.     Time        Source            Destination       Protocol Length Info
    157 251.281828  192.168.232.215   192.168.232.176   NBNS     104 Name query response NB 192.168.232.215
    158 251.281834  192.168.232.176   192.168.232.215   NBNS     104 Registration response, Name is in conflict NB 192.168.232.148
    161 252.282406  192.168.232.215   192.168.232.176   NBNS     104 Name query response NB 192.168.232.215
    166 254.178011  192.168.232.215   192.168.232.176   MDNS      83 Standard query response 0x0000 A 192.168.232.215
    167 254.178176  192.168.232.215   192.168.232.176   NBNS     104 Name query response NB 192.168.232.215
    170 254.179997  192.168.232.215   192.168.232.176   MDNS      95 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
    171 254.182306  192.168.232.215   192.168.232.176   LLMNR     90 Standard query response 0x4a65 A prinetr A 192.168.232.215
    172 254.186728  192.168.232.215   192.168.232.176   LLMNR    102 Standard query response 0x5ae5 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
    183 254.228659  192.168.232.215   192.168.232.176   MDNS      83 Standard query response 0x0000 A 192.168.232.215
    184 254.230005  192.168.232.215   192.168.232.176   MDNS      95 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
    187 254.233162  192.168.232.215   192.168.232.176   LLMNR     90 Standard query response 0x3188 A prinetr A 192.168.232.215
    188 254.237206  192.168.232.215   192.168.232.176   LLMNR    102 Standard query response 0x567d AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
    191 254.243264  192.168.232.215   192.168.232.176   MDNS      83 Standard query response 0x0000 A 192.168.232.215
    193 254.244371  192.168.232.215   192.168.232.176   MDNS      95 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
    195 254.247641  192.168.232.215   192.168.232.176   LLMNR     90 Standard query response 0x02c2 A prinetr A 192.168.232.215
    196 254.251873  192.168.232.215   192.168.232.176   LLMNR    102 Standard query response 0xb232 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:3313
```

```
▸ Frame 75: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
▸ Ethernet II, Src: VMware_44:ca:ef (00:0c:29:44:ca:ef), Dst: VMware_fa:cb:e9 (00:0c:29:fa:cb:e9)
▸ Internet Protocol Version 4, Src: 192.168.232.215, Dst: 192.168.232.162
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (response)
```

```
0000  00 0c 29 fa cb e9 00 0c  29 44 ca ef 08 00 45 00   ··)····· )D····E·
0010  00 48 da b3 40 00 40 11  0d 26 c0 a8 e8 d7 c0 a8   ·H··@·@· ·&······
0020  e8 a2 14 e9 14 e9 00 34  10 f8 00 00 84 00 00 00   ·······4 ········
0030  00 01 00 00 00 00 0a 66  69 6c 65 73 68 61 61 72   ·······f ileshaar
0040  65 05 6c 6f 63 61 6c 00  00 01 00 01 00 00 00 78   e·local· ·······x
0050  00 04 c0 a8 e8 d7                                  ······
```

Q4

Follow stream > filter
Jane smith



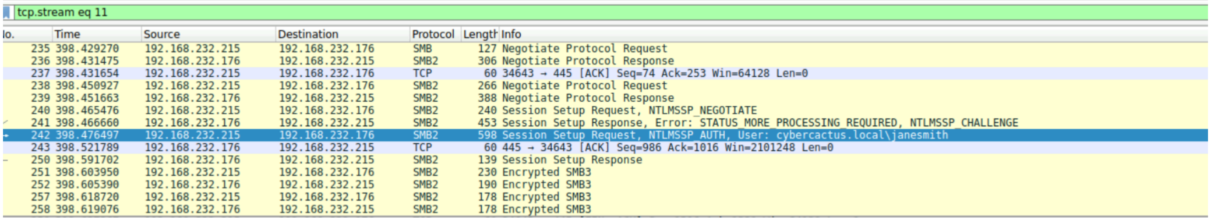
Wireshark · Follow TCP Stream (tcp.stream eq 11) · PoisonedCredentials.pcap

```
...E.SMBr....................@B....."..NT LM 0.12..SMB 2.002..SMB 2.???......SMB@.....................................................
.......A.............ZO...ZS..\................P...]............x.....`v..+......l0j.<0:.
+.....7....             *.H....... *.H.......
*.H........
+.....7..
.*0(.&.$not_defined_in_RFC4178@please_ignore.....SMB@.........................................................$.......@.........[..]
.r..O.p....................&....... ....<]..^z..j:3.Q......;aCf.l..p.......
..............................................J.SMB@.............................................................A.............ZO...ZS
..\................
...]............x.....`v..+......l0j.<0:.
+.....7....             *.H....... *.H.......
*.H........
+.....7..
.*0(.&.$not_defined_in_RFC4178@please_ignore..&....... ... ..&.%.2..i*....r.....F..W..$.!....................
.....................SMB@...........................................................................X.^.........`\..+......R0P..0..
+.....7..
.>.<NTLMSSP.....5....... .......1...cybercactus.localWORKSTATION.....SMB@....................................@................. .
..H.C....?0..;..
.....
+.....7..
...$... NTLMSSP.........8...5.....^K|.v.............N...
.aJ....C.Y.B.E.R.C.A.C.T.U.S.....C.Y.B.E.R.C.A.C.T.U.S.....A.C.C.O.U.N.T.I.N.G.P.C...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...<.A.c.c.o.u
.n.t.i.n.g.P.C...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.....!...]............SMB@...................
...................@.............................X...............0...........NTLMSSP.........@.......X..."."..Z.......|.............
.....5...u;.X.L$.$/...ZvwCe(..4*........j..;.."...........0..]...Ce(..4*.........C.Y.B.E.R.C.A.C.T.U.S.....A.C.C.O.U.N.T.I.N.G.P.C..."
.c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...<.A.c.c.o.u.n.t.i.n.g.P.C...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a
.l.....!...]..........c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.j.a.n.e.s.m.i.t.h.W.O.R.K.S.T.A.T.I.O.N....j8....0.?./AU...Q.SMB@..........
...........................@.........1_D.D}          .          ...H.      ...0...
.......SMB3RF<q....'..m]=....2S..il.......x...........@.....c.."|{,.L.....:2...$....N.U.+`.S@.     )..l..J..:.;V0%_...4...         \
....K..;/.....B...J.A.Z.O.
F.U_...VV.X8..f.4,....1+Y...}Q.....SMB..{t...!..3......&.I[...........P...........@.....`..e..u$.......M.....Q.[.H..M....+....".21..x
..L...Y4.9J..b...
.H.W.....yb.\....x.SMB....X8.j..S.x..K....}.d.q;......D............@.........P.\.k.J...}!..Y............f.../k.D.
```

Packet 252. 6 client pkt(s), 6 server pkt(s), 11 turn(s). Click to select.

Entire conversation (2645 bytes) | Show data as ASCII | Stream 11

Find: | Find Next



tcp.stream eq 11

```
No.  Time        Source           Destination      Protocol Length Info
 235 398.429270  192.168.232.215  192.168.232.176  SMB      127 Negotiate Protocol Request
 236 398.431475  192.168.232.176  192.168.232.215  SMB2     306 Negotiate Protocol Response
 237 398.431654  192.168.232.215  192.168.232.176  TCP       60 34643 → 445 [ACK] Seq=74 Ack=253 Win=64128 Len=0
 238 398.450927  192.168.232.215  192.168.232.176  SMB2     266 Negotiate Protocol Request
 239 398.451663  192.168.232.176  192.168.232.215  SMB2     388 Negotiate Protocol Response
 240 398.465476  192.168.232.215  192.168.232.176  SMB2     240 Session Setup Request, NTLMSSP_NEGOTIATE
 241 398.466660  192.168.232.176  192.168.232.215  SMB2     453 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
 242 398.476497  192.168.232.215  192.168.232.176  SMB2     598 Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith
 243 398.521789  192.168.232.176  192.168.232.215  TCP       60 445 → 34643 [ACK] Seq=986 Ack=1016 Win=2101248 Len=0
 250 398.591702  192.168.232.176  192.168.232.215  SMB2     139 Session Setup Response
 251 398.603950  192.168.232.215  192.168.232.176  SMB2     230 Encrypted SMB3
 252 398.605390  192.168.232.176  192.168.232.215  SMB2     190 Encrypted SMB3
 257 398.618720  192.168.232.215  192.168.232.176  SMB2     178 Encrypted SMB3
 258 398.619076  192.168.232.176  192.168.232.215  SMB2     178 Encrypted SMB3
```

Q5

Q5 192.168.232.215 with SMB protocol> Follow stream > filter >AccountingPC