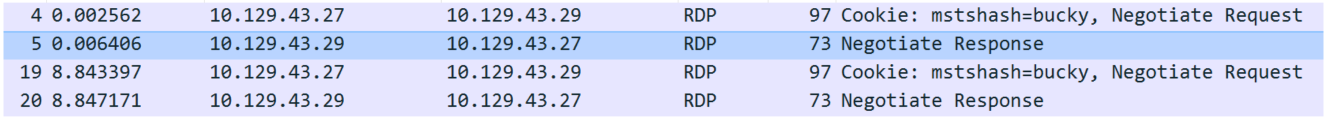
Wireshark – RDP Decryption

The given capture file is opened.

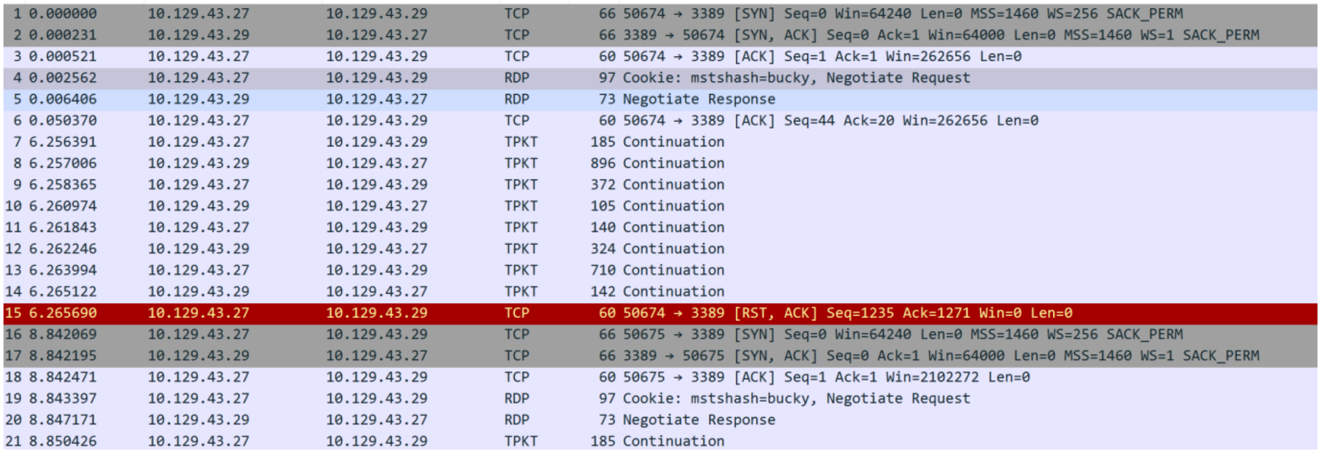
The capture is filtered for RDP for easier inspection.



```
 4 0.002562    10.129.43.27    10.129.43.29    RDP     97 Cookie: mstshash=bucky, Negotiate Request
 5 0.006406    10.129.43.29    10.129.43.27    RDP     73 Negotiate Response
19 8.843397    10.129.43.27    10.129.43.29    RDP     97 Cookie: mstshash=bucky, Negotiate Request
20 8.847171    10.129.43.29    10.129.43.27    RDP     73 Negotiate Response
```

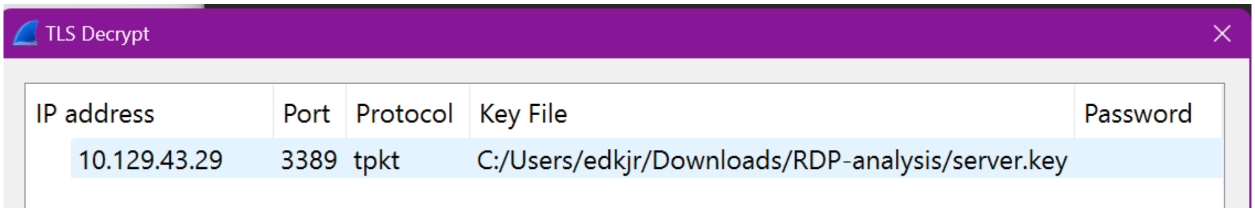
Due to RDP using TLS to encrypt data, not much can be gathered from the capture.

Filtering the capture using “tcp.port == 3389” confirms that several packets were sent using RDP but can’t be investigated due to encryption.



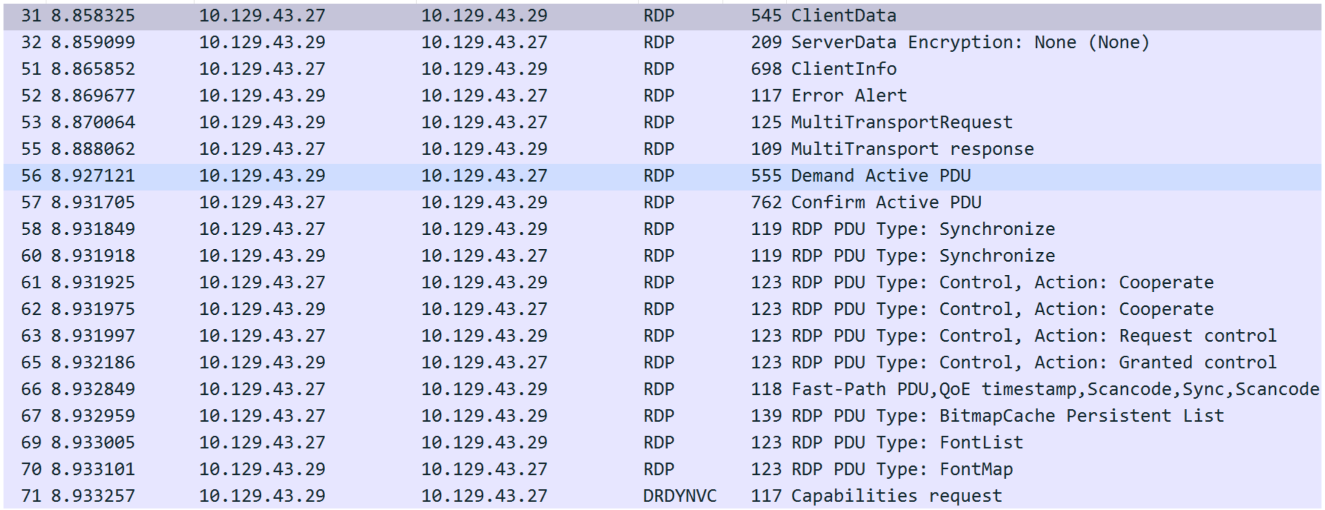
```
 1 0.000000    10.129.43.27    10.129.43.29    TCP     66 50674 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 2 0.000231    10.129.43.29    10.129.43.27    TCP     66 3389 → 50674 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
 3 0.000521    10.129.43.27    10.129.43.29    TCP     60 50674 → 3389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
 4 0.002562    10.129.43.27    10.129.43.29    RDP     97 Cookie: mstshash=bucky, Negotiate Request
 5 0.006406    10.129.43.29    10.129.43.27    RDP     73 Negotiate Response
 6 0.050370    10.129.43.27    10.129.43.29    TCP     60 50674 → 3389 [ACK] Seq=44 Ack=20 Win=262656 Len=0
 7 6.256391    10.129.43.27    10.129.43.29    TPKT   185 Continuation
 8 6.257006    10.129.43.29    10.129.43.27    TPKT   896 Continuation
 9 6.258365    10.129.43.27    10.129.43.29    TPKT   372 Continuation
10 6.260974    10.129.43.29    10.129.43.27    TPKT   105 Continuation
11 6.261843    10.129.43.27    10.129.43.29    TPKT   140 Continuation
12 6.262246    10.129.43.29    10.129.43.27    TPKT   324 Continuation
13 6.263994    10.129.43.27    10.129.43.29    TPKT   710 Continuation
14 6.265122    10.129.43.29    10.129.43.27    TPKT   142 Continuation
15 6.265690    10.129.43.27    10.129.43.29    TCP     60 50674 → 3389 [RST, ACK] Seq=1235 Ack=1271 Win=0 Len=0
16 8.842069    10.129.43.27    10.129.43.29    TCP     66 50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 8.842195    10.129.43.29    10.129.43.27    TCP     66 3389 → 50675 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
18 8.842471    10.129.43.27    10.129.43.29    TCP     60 50675 → 3389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
19 8.843397    10.129.43.27    10.129.43.29    RDP     97 Cookie: mstshash=bucky, Negotiate Request
20 8.847171    10.129.43.29    10.129.43.27    RDP     73 Negotiate Response
21 8.850426    10.129.43.27    10.129.43.29    TPKT   185 Continuation
```

Under the Preferences section of Wireshark, the the given key can be added for decryption when the TLS protocol is used.



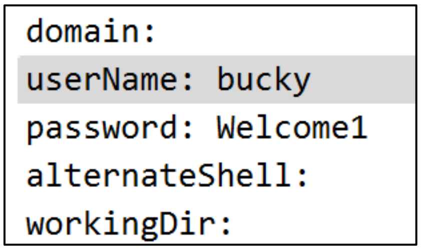
IP address	Port	Protocol	Key File	Password
10.129.43.29	3389	tpkt	C:/Users/edkjr/Downloads/RDP-analysis/server.key	

After refreshing the capture, the contents of the RDP packets can now be viewed in plaintext.



```
31 8.858325    10.129.43.27    10.129.43.29    RDP      545 ClientData
32 8.859099    10.129.43.29    10.129.43.27    RDP      209 ServerData Encryption: None (None)
51 8.865852    10.129.43.27    10.129.43.29    RDP      698 ClientInfo
52 8.869677    10.129.43.29    10.129.43.27    RDP      117 Error Alert
53 8.870064    10.129.43.29    10.129.43.27    RDP      125 MultiTransportRequest
55 8.888062    10.129.43.27    10.129.43.29    RDP      109 MultiTransport response
56 8.927121    10.129.43.29    10.129.43.27    RDP      555 Demand Active PDU
57 8.931705    10.129.43.27    10.129.43.29    RDP      762 Confirm Active PDU
58 8.931849    10.129.43.27    10.129.43.29    RDP      119 RDP PDU Type: Synchronize
60 8.931918    10.129.43.29    10.129.43.27    RDP      119 RDP PDU Type: Synchronize
61 8.931925    10.129.43.27    10.129.43.29    RDP      123 RDP PDU Type: Control, Action: Cooperate
62 8.931975    10.129.43.29    10.129.43.27    RDP      123 RDP PDU Type: Control, Action: Cooperate
63 8.931997    10.129.43.27    10.129.43.29    RDP      123 RDP PDU Type: Control, Action: Request control
65 8.932186    10.129.43.29    10.129.43.27    RDP      123 RDP PDU Type: Control, Action: Granted control
66 8.932849    10.129.43.27    10.129.43.29    RDP      118 Fast-Path PDU,QoE timestamp,Scancode,Sync,Scancode
67 8.932959    10.129.43.27    10.129.43.29    RDP      139 RDP PDU Type: BitmapCache Persistent List
69 8.933005    10.129.43.27    10.129.43.29    RDP      123 RDP PDU Type: FontList
70 8.933101    10.129.43.29    10.129.43.27    RDP      123 RDP PDU Type: FontMap
71 8.933257    10.129.43.29    10.129.43.27    DRDYNVC  117 Capabilities request
```

When inspecting the details of the ClientInfo packet, we find communication with this server was made using the account with username “bucky”



```
domain:
userName: bucky
password: Welcome1
alternateShell:
workingDir:
```