

Account Name:

Logon ID:

Process ID: Process Name:

Detailed Authentication Information:

Transited Services:

Account Domain:

Linked Logon ID:

Network Account Name:

Network Account Domain: -

Workstation Name: WIN10-1703

Logon Process: User32
Authentication Package: Negotiate

Package Name (NTLM only): Key Length: 0

Source Network Address: 10.0.0.15

{7325c0ac-0b1d-0c8f-8aae-7fad6d69d4d8}

C:\Windows\System32\svchost.exe

Security ID:

Logon ID:

Account Domain:

Linked Logon ID:

Process ID: Process Name:

Network Information:

Network Account Name:

Network Account Domain: -

Detailed Authentication Information:

Logon Process: User32

Package Name (NTLM only): Key Length: 0

Transited Services:

Workstation Name: WIN10-1703

Source Network Address: 10.0.0.130

Authentication Package: Negotiate

C:\Windows\System32\svchost.exe

Account Name:

Logon GUID:

Process ID: Process Name:

Network Information:

Account Domain:

Linked Logon ID:

Network Account Name:

Network Account Domain: -

Workstation Name: WIN10-1703

Source Network Address: 127.0.0.1

Source Port: 0

Logon Process: User32

Transited Services: Package Name (NTLM only):
Key Length: 0

Authentication Package: Negotiate

C:\Windows\System32\svchost.exe

Linked Logon ID:

Process ID:

Network Information:

Process Name:

Workstation Name:

Detailed Authentication Information:

Network Account Name:

Network Account Domain: -

Source Port: 49208

Logon Process: Kerberos
Authentication Package: Kerberos
Transited Services: Package Name (NTLM only): Key Length: 0

Source Network Address: fe80::6d6b:8141:e4ff:6a50

S-1-5-21-1913345275-1711810662-261465553-5

{fa4ecac3-35ab-e1c6-e8e7-d51d5461841e}

0x53c C:\Windows\System32\svchost.exe

Account Name:

Account Domain: Logon ID:

Logon GUID:

Process ID: Process Name:

Network Information:

Linked Logon ID:

Network Account Name:

Network Account Domain:

Workstation Name: 2016DC

Source Network Address: 127.0.0.1

Logon Process: User32
Authentication Package: Negotiate

Source Port: 0

Package Name (NTLM only): Key Length: 0

Detailed Authentication Information:

administrator HQCORP 0x26FCEC

C:\Windows\System32\inetsrv\w3wp.exe

Account Domain:

Linked Logon ID:

Logon GUID:

Process ID:

Network Information:

Process Name:

Network Account Name:

Network Account Domain: -

Workstation Name: 2016DC

Source Port: 49703

Detailed Authentication Information:

Logon Process: Advapi

Package Name (NTLM only): Key Length: 0

Transited Services:

Source Network Address: 10.0.0.130

Authentication Package: Negotiate



Special thanks to Andrei Miroshnikov for awesome book "Windows Security Monitoring: Scenarios and Patterns" https://www.amazon.com/gp/product/B07BGHYF61