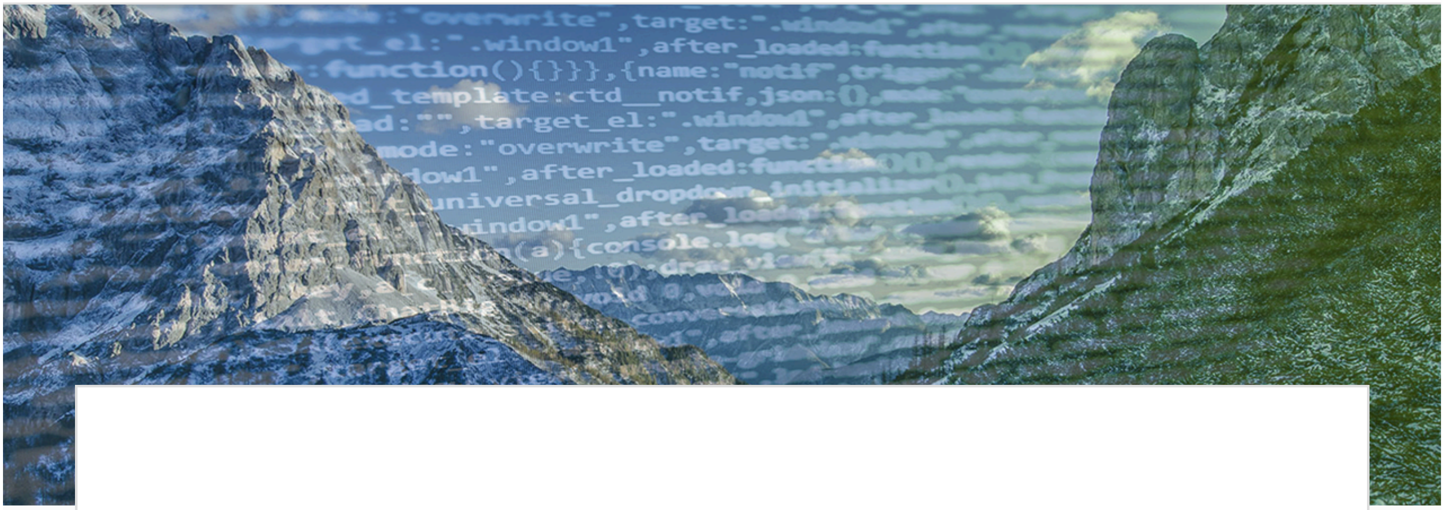
Ponder The Bits

Musings and confusings. All things DFIR.



Windows RDP-Related Event Logs: Identification, Tracking, and Investigation

BY JONATHON POLING / ON FEBRUARY 20, 2018 / IN EVENT LOGS, FORENSICS, INCIDENT RESPONSE, RDP, REMOTE DESKTOP, UNCATEGORIZED, WINDOWS

Early in my DFIR career, I struggled with understanding how exactly to identify and understand all the RDP-related Windows Event Logs. I would read a few things here and there, think I understood it, then move on to the next case – repeating the same loop over and over again and never really acquiring full comprehension. That is until one day I finally got tired of repeating the same questions/research and just made a cheat sheet laying out the most common RDP-related Event ID's that I'd encountered along with their relevance and descriptions. From that point on, as I sporadically encountered related questions/confusion from others in the community, I would simply refer to my cheat sheet to provide an immediate response or clarification – saving them from the hours of repeated questioning and research I had already done.

However, it seems the community continues to encounter the same struggle in identifying and understanding RDP-related Windows Event Log ID's, where each is located, and even what some of them mean (no thanks to some of Microsoft's very confusing documentation and descriptions). As such, I recently set out to try and find an easy route to the solution for this problem (i.e. hopefully find a single website to point to with all this information). Though I've found parts of the answer in posts here and there, each of them were missing parts of the puzzle (either missing ID's, descriptions, explanations, and/or overall how they fit together in a chronological fashion). I will say JPCERTCC did an awesome job capturing a ton of information here, I just can't quite decipher or discern the clear order of events and some appear out of order (at least how I have encountered them, but maybe I'm reading it wrong…). At any rate, as they say, necessity is the mother of invention.

So, I decided to create a blog post that I hope can serve as a succinct one-stop shop for understanding and identifying the most commonly encountered and empirically useful* RDP-related Windows Event Log ID's/entries for tracking and investigating RDP usage on a Windows Vista+ endpoint. The Windows Event ID's in the XP days were different than those in Vista+ Operating Systems. So, I decided to leave those out for now, but perhaps I will add them in the future.

*Yes, there are Event ID's like 1146, 1147, and 1148 which look great in Microsoft's documentation as a very useful source of information. However, I've yet to see (m)any of these commonly occurring in the wild.

I debated back and forth on the best way to sort/group these. Ultimately, in truly pragmatic fashion, I figured it would likely be most useful to sort them in the (chronological) order in which you might expect to find them. Ergo, the flow/section breakup is the following:

Network Connection

->-> Authentication

->-> Logon

->-> Session Disconnect/Reconnect

->-> Logoff

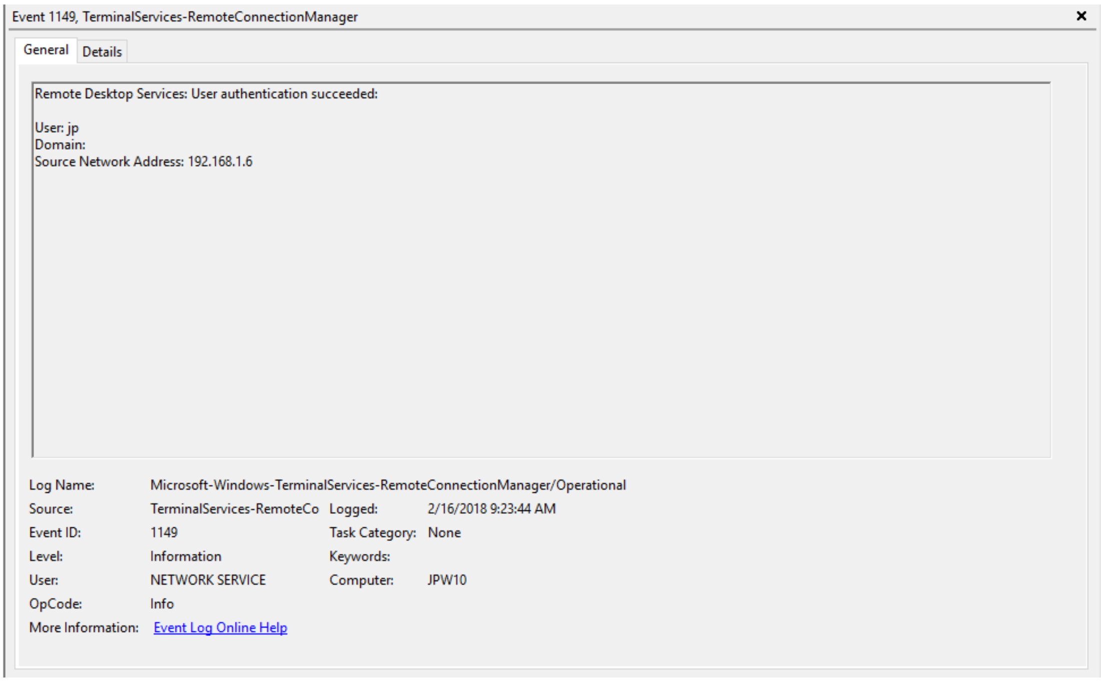
Network Connection

This section covers the first indications of an RDP logon – the initial network connection to a machine.

Log: Microsoft-Windows-Terminal-Services-RemoteConnectionManager/Operational

Log Location: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

Event ID: 1149
Provider Name: Microsoft-Windows-Terminal-Services-RemoteConnectionManager
Description: "User authentication succeeded"
Notes: Despite this seemingly clear-cut description, this event actually DOES NOT indicate a successful user authentication in the sense that many might expect (e.g., successful input and acceptance of a username and password). Instead, "authentication" in this sense is referring to successful network authentication, as in someone successfully executed an RDP network connection to the target machine and it successfully responded and displayed a login window for the next step of entering credentials. For example, if I launched the RDP Desktop Connection program on my computer, input a target IP, and hit enter, it would simply display the target system's screen and produce an 1149 Event ID indicating I had successfully connected to the target, WELL BEFORE I even entered any credentials. So, repeat after me, *"An Event ID 1149 DOES NOT indicate successful authentication to a target, simply a successful RDP network connection"*.
TL;DR: NOT AN AUTHENTICATION. Someone launched an RDP client, specified the target machine (possibly with a username and domain), and hit enter to make a successful network connection to the target. Nothing more, nothing less.

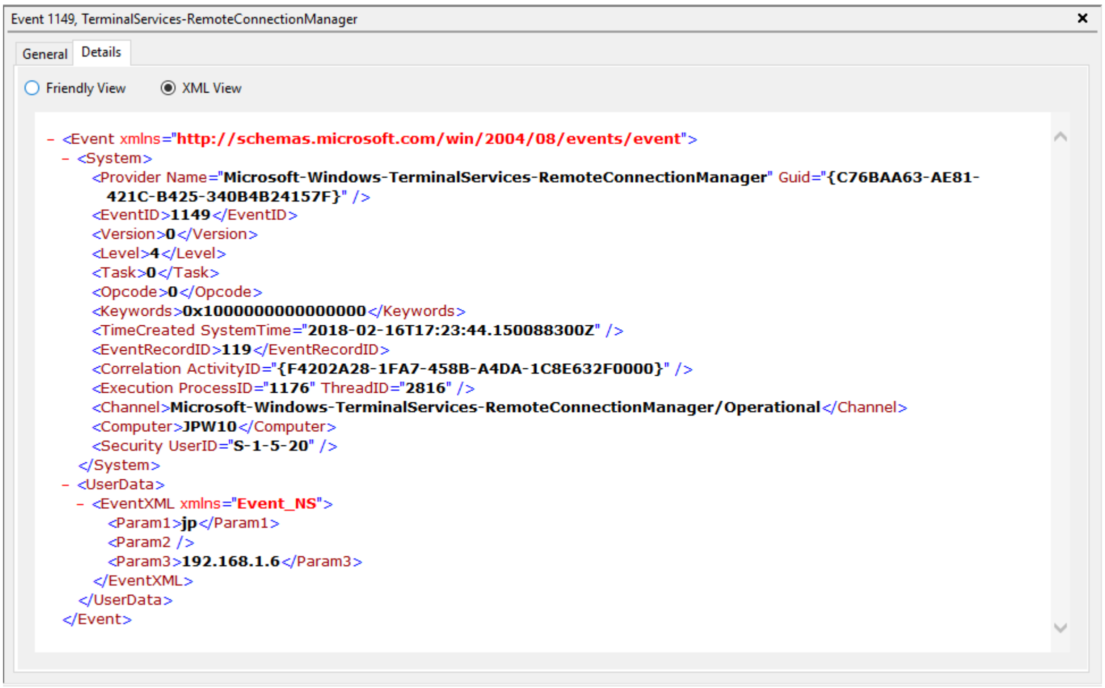


Event 1149, TerminalServices-RemoteConnectionManager

Remote Desktop Services: User authentication succeeded:

User: jp
Domain:
Source Network Address: 192.168.1.6

Log Name:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational		
Source:	TerminalServices-RemoteCo	Logged:	2/16/2018 9:23:44 AM
Event ID:	1149	Task Category:	None
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		



Event 1149, TerminalServices-RemoteConnectionManager

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-RemoteConnectionManager" Guid="{C76BAA63-AE81-
        421C-B425-340B4B24157F}" />
      <EventID>1149</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T17:23:44.150088300Z" />
      <EventRecordID>119</EventRecordID>
      <Correlation ActivityID="{F4202A28-1FA7-458B-A4DA-1C8E632F0000}" />
      <Execution ProcessID="1176" ThreadID="2816" />
      <Channel>Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-20" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <Param1>jp</Param1>
        <Param2 />
        <Param3>192.168.1.6</Param3>
      </EventXML>
    </UserData>
  </Event>
```

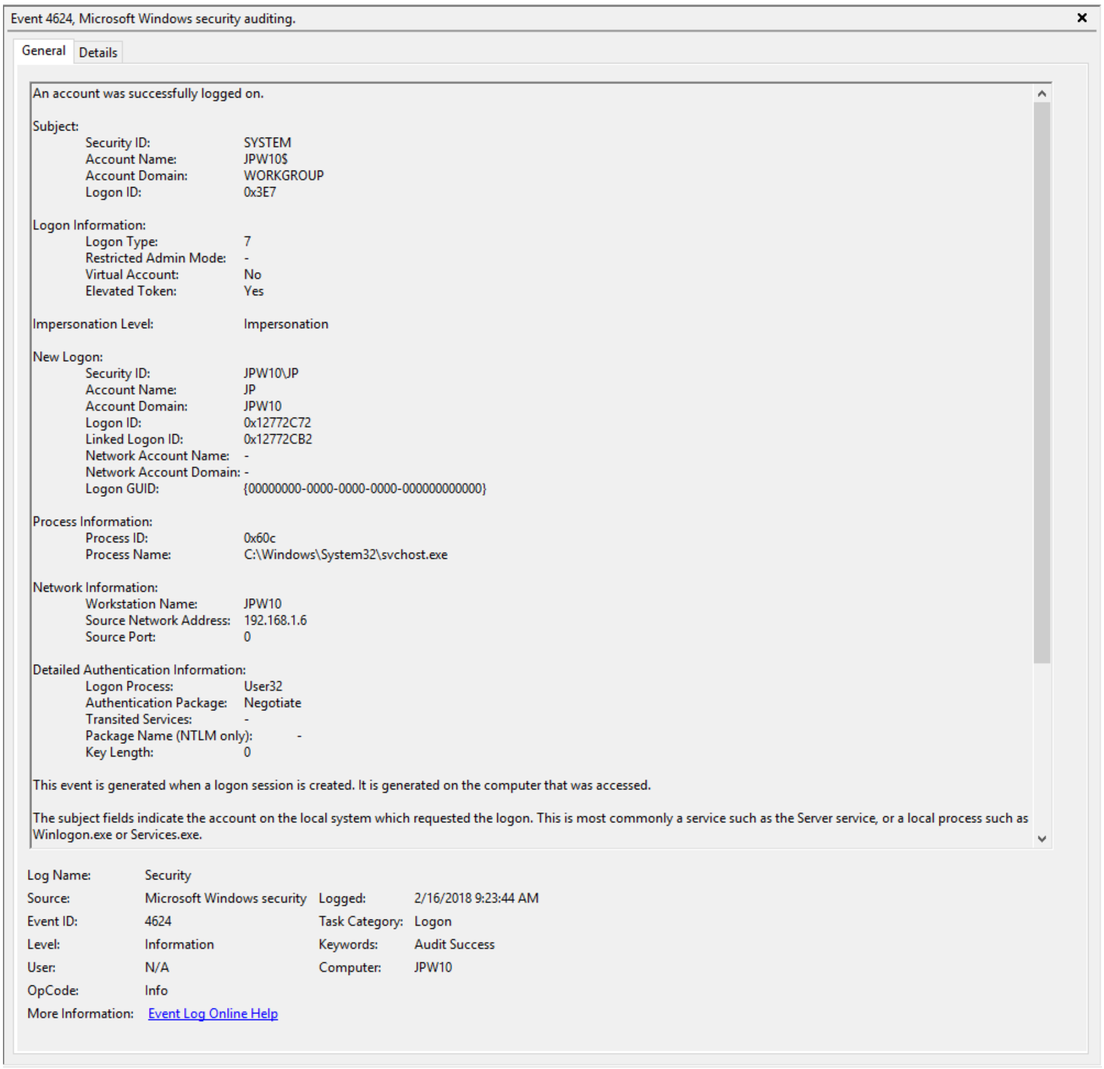
Authentication

This section covers the authentication portion of the RDP connection – whether or not the logon is allowed based on success/failure of username/password combo.

Log: Security

Log Location:
%SystemRoot%\System32\Winevt\Logs\Security.evtx

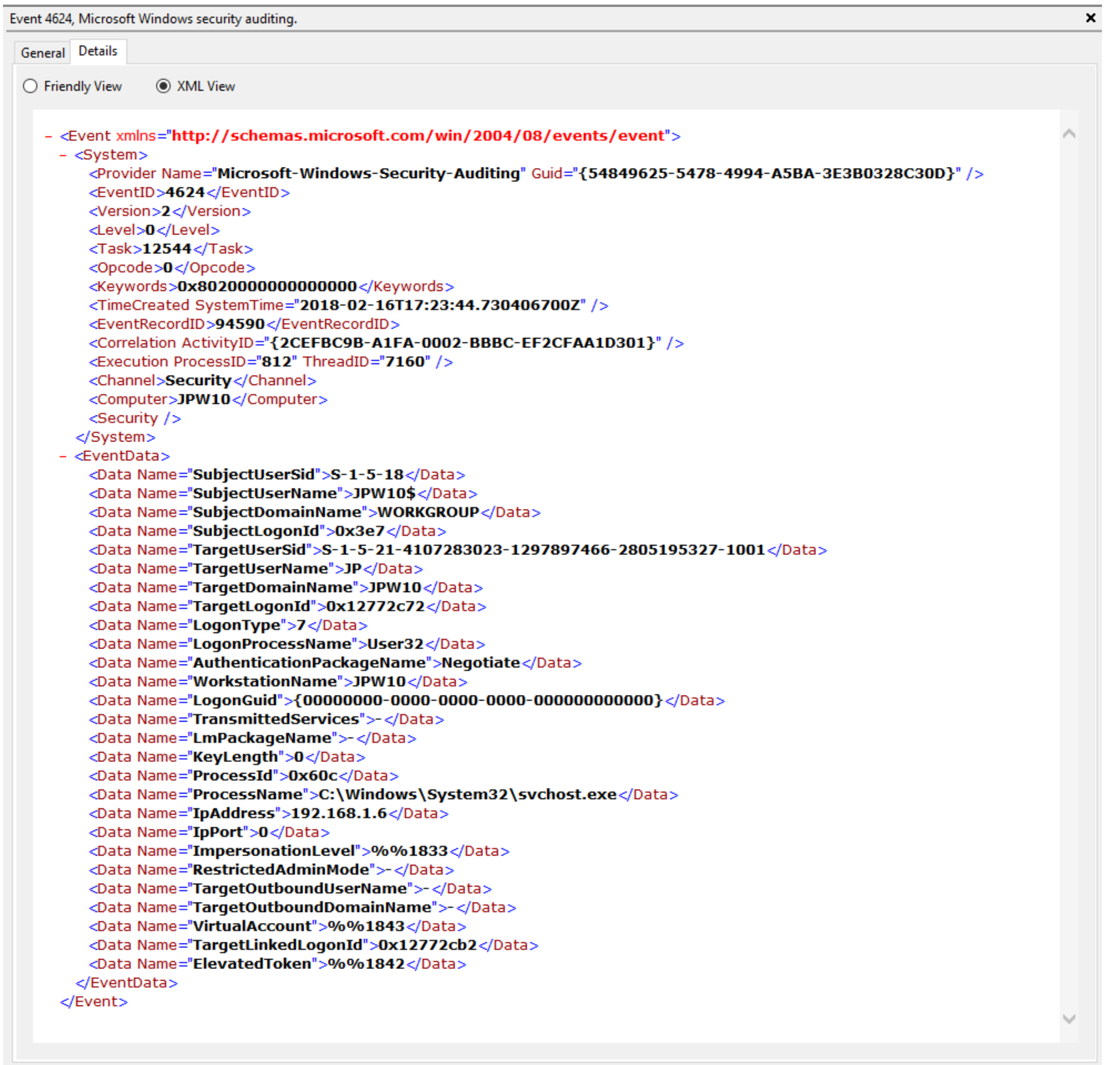
Event ID: 4624
Provider Name: Microsoft-Windows-Security-Auditing
LogonType: Type 3 (Network) when NLA is Enabled (and at times even when it's not) followed by Type 10 (RemoteInteractive / a.k.a. Terminal Services / a.k.a. Remote Desktop) *OR* Type 7 from a Remote IP (if it's a reconnection from a previous/existing RDP session)
Description: "An account was successfully logged on"
Notes: I thought this one was pretty straight forward – just look for Type 10 logons for RDP. However, in a bit more research, I discovered that often a Type 3 logon (for NLA) will occur prior to the Type 10 logon. In addition, I also discovered that RDP'ing to a system of which you'd previously RDP'ed and not formally logged off/out would instead yield a Logon Type 7 logon versus the Logon Type 10 we'd expect. This makes sense in a way in that a Logon Type 7 ("This workstation was unlocked") is essentially what is happening. However, to delineate this from non-RDP Type 7 logons in which a person was sitting at the machine and just unlocked the machine, we can look for remote non-local IP's in the IpAddress field.
TL;DR: User successfully logged on to this system with the specified *TargetUserName* and *TargetDomainName* from the specified *IpAddress*.



Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           JPW10$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             7
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            JPW10\JP
        Account Name:           JP
        Account Domain:         JPW10
        Logon ID:               0x12772C72
        Linked Logon ID:        0x12772CB2
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x60c
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       JPW10
        Source Network Address: 192.168.1.6
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as
Winlogon.exe or Services.exe.
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         2/16/2018 9:23:44 AM
Event ID:          4624                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       JPW10
OpCode:            Info
More Information:  Event Log Online Help
```

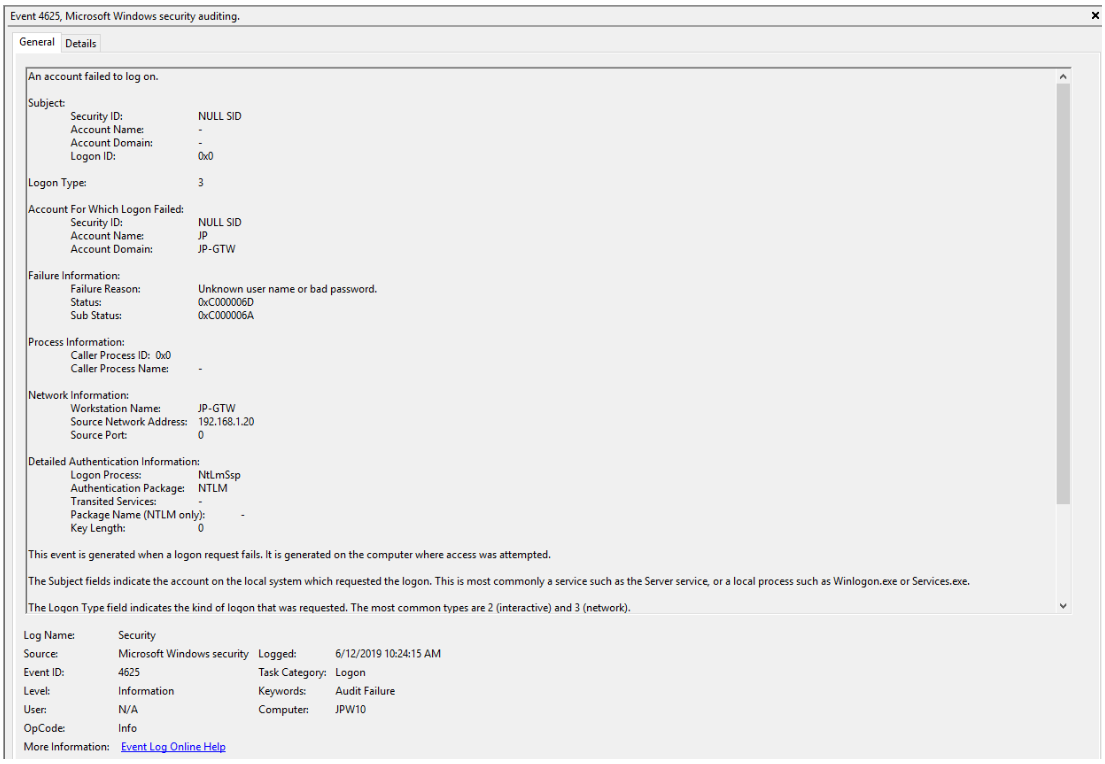


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
      <EventID>4624</EventID>
      <Version>2</Version>
      <Level>0</Level>
      <Task>12544</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8020000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T17:23:44.730406700Z" />
      <EventRecordID>94590</EventRecordID>
      <Correlation ActivityID="{2CEFBC9B-A1FA-0002-BBBC-EF2CFAA1D301}" />
      <Execution ProcessID="812" ThreadID="7160" />
      <Channel>Security</Channel>
      <Computer>JPW10</Computer>
      <Security />
    </System>
  - <EventData>
      <Data Name="SubjectUserSid">S-1-5-18</Data>
      <Data Name="SubjectUserName">JPW10$</Data>
      <Data Name="SubjectDomainName">WORKGROUP</Data>
      <Data Name="SubjectLogonId">0x3e7</Data>
      <Data Name="TargetUserSid">S-1-5-21-4107283023-1297897466-2805195327-1001</Data>
      <Data Name="TargetUserName">JP</Data>
      <Data Name="TargetDomainName">JPW10</Data>
      <Data Name="TargetLogonId">0x12772c72</Data>
      <Data Name="LogonType">7</Data>
      <Data Name="LogonProcessName">User32</Data>
      <Data Name="AuthenticationPackageName">Negotiate</Data>
      <Data Name="WorkstationName">JPW10</Data>
      <Data Name="LogonGuid">{00000000-0000-0000-0000-000000000000}</Data>
      <Data Name="TransmittedServices">-</Data>
      <Data Name="LmPackageName">-</Data>
      <Data Name="KeyLength">0</Data>
      <Data Name="ProcessId">0x60c</Data>
      <Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>
      <Data Name="IpAddress">192.168.1.6</Data>
      <Data Name="IpPort">0</Data>
      <Data Name="ImpersonationLevel">%%1833</Data>
      <Data Name="RestrictedAdminMode">-</Data>
      <Data Name="TargetOutboundUserName">-</Data>
      <Data Name="TargetOutboundDomainName">-</Data>
      <Data Name="VirtualAccount">%%1843</Data>
      <Data Name="TargetLinkedLogonId">0x12772cb2</Data>
      <Data Name="ElevatedToken">%%1842</Data>
    </EventData>
</Event>
```

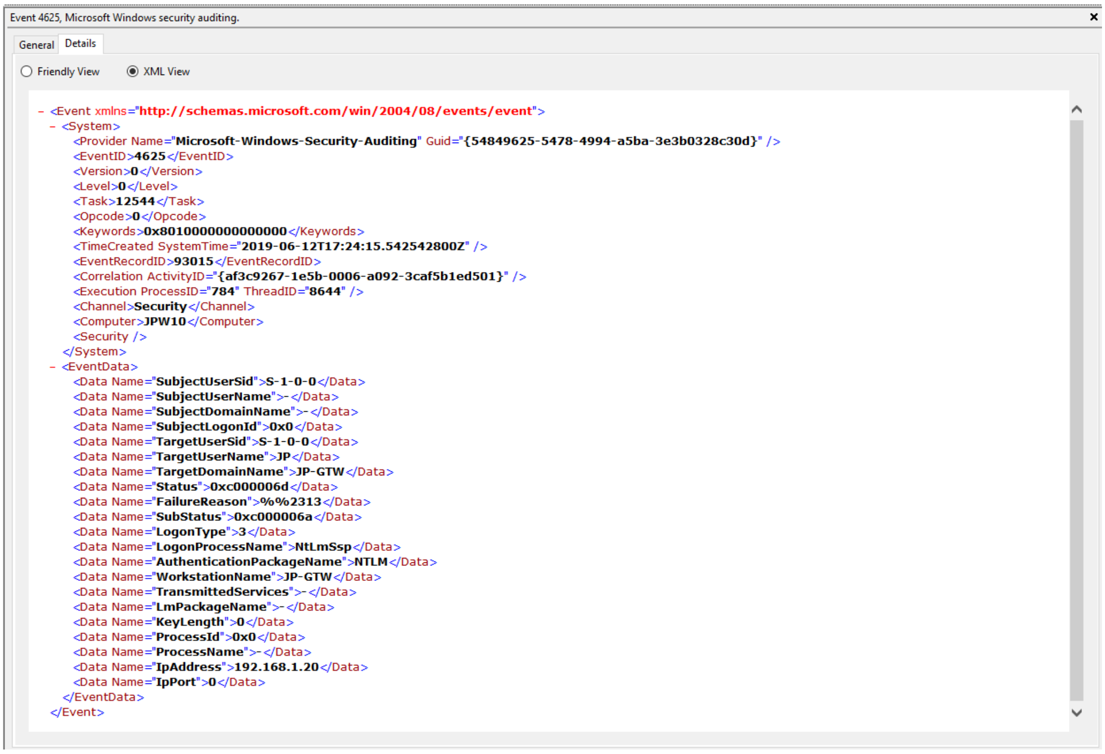
Event ID: 4625
Provider Name: Microsoft-Windows-Security-Auditing
LogonType: Type 3 (Network) when NLA is Enabled (and at times even when it's not) *and/or* Type 10 (RemoteInteractive / a.k.a. Terminal Services / a.k.a. Remote Desktop)
Description: "An account failed to log on"
Notes: Why do we care about failures? Well, this is helpful in identifying (brute force) failure attempts and seeing when/where an attacker may be attempting stolen/compromised credentials. The Status/Sub Status Code will also be helpful in delineating legitimate failures (e.g. "expired password") as well as possibly providing insight into attacker activity (e.g. repetitive "user name does not exist" codes

could indicate brute force guessing by a tool and/or a more targeted lack of username knowledge/awareness in the environment by the attacker).

TL;DR: User failed to log on to this system with the specified TargetUserName and TargetDomainName from the specified IpAddress.



```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           JP
        Account Domain:         JP-GTW

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       JP-GTW
        Source Network Address: 192.168.1.20
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

Log Name:      Security
Source:        Microsoft Windows security   Logged:        6/12/2019 10:24:15 AM
Event ID:      4625                         Task Category: Logon
Level:         Information                  Keywords:      Audit Failure
User:          N/A                          Computer:      JPW10
OpCode:        Info
More Information: Event Log Online Help
```



Event 4625, Microsoft Windows security auditing.

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-3e3b0328c30d}" />
      <EventID>4625</EventID>
      <Version>0</Version>
      <Level>0</Level>
      <Task>12544</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8010000000000000</Keywords>
      <TimeCreated SystemTime="2019-06-12T17:24:15.542542800Z" />
      <EventRecordID>93015</EventRecordID>
      <Correlation ActivityID="{af3c9267-1e5b-0006-a092-3caf5b1ed501}" />
      <Execution ProcessID="784" ThreadID="8644" />
      <Channel>Security</Channel>
      <Computer>JPW10</Computer>
      <Security />
    </System>
  - <EventData>
      <Data Name="SubjectUserSid">S-1-0-0</Data>
      <Data Name="SubjectUserName">-</Data>
      <Data Name="SubjectDomainName">-</Data>
      <Data Name="SubjectLogonId">0x0</Data>
      <Data Name="TargetUserSid">S-1-0-0</Data>
      <Data Name="TargetUserName">JP</Data>
      <Data Name="TargetDomainName">JP-GTW</Data>
      <Data Name="Status">0xc000006d</Data>
      <Data Name="FailureReason">%%2313</Data>
      <Data Name="SubStatus">0xc000006a</Data>
      <Data Name="LogonType">3</Data>
      <Data Name="LogonProcessName">NtLmSsp</Data>
      <Data Name="AuthenticationPackageName">NTLM</Data>
      <Data Name="WorkstationName">JP-GTW</Data>
      <Data Name="TransmittedServices">-</Data>
      <Data Name="LmPackageName">-</Data>
      <Data Name="KeyLength">0</Data>
      <Data Name="ProcessId">0x0</Data>
      <Data Name="ProcessName">-</Data>
      <Data Name="IpAddress">192.168.1.20</Data>
      <Data Name="IpPort">0</Data>
    </EventData>
  </Event>
```

#ProTip(s):

1) When NLA is enabled, a failed RDP logon (due to wrong username, password, etc.) will result in a 4625 Type 3 failure. When NLA is not enabled, you *should* see a 4625 Type 10 failure.

2) Both of these entries also contain a "SubjectLogonID" or a "TargetLogonID" field. This ID is unique for each logon session and is also present in various other Event Log entries, making it theoretically useful for tracking/delineating a specific user's activities, particularly on systems allowing multiple logged on users. However, do take note that a unique *LogonID is assigned for each session, meaning if a user connects, then disconnects (without logging out, thus simply ending the current session), then reconnects (i.e. starting a new session), they will be assigned a different unique *LogonID. All to say that a single user(name) may have multiple unique *LogonID's to track depending how many sessions they've instantiated, not to mention Windows makes it very confusing

sometimes with multiple 4624's with different *LogonID's for the same session. So, YMMV.

Additional References:

David Cowen's Forensic Lunch Test Kitchen – RDP Testing (1 , 2 , 3)
Microsoft Forum Answer Re: RDP 4624 Type 3 Logons (link)

Logon

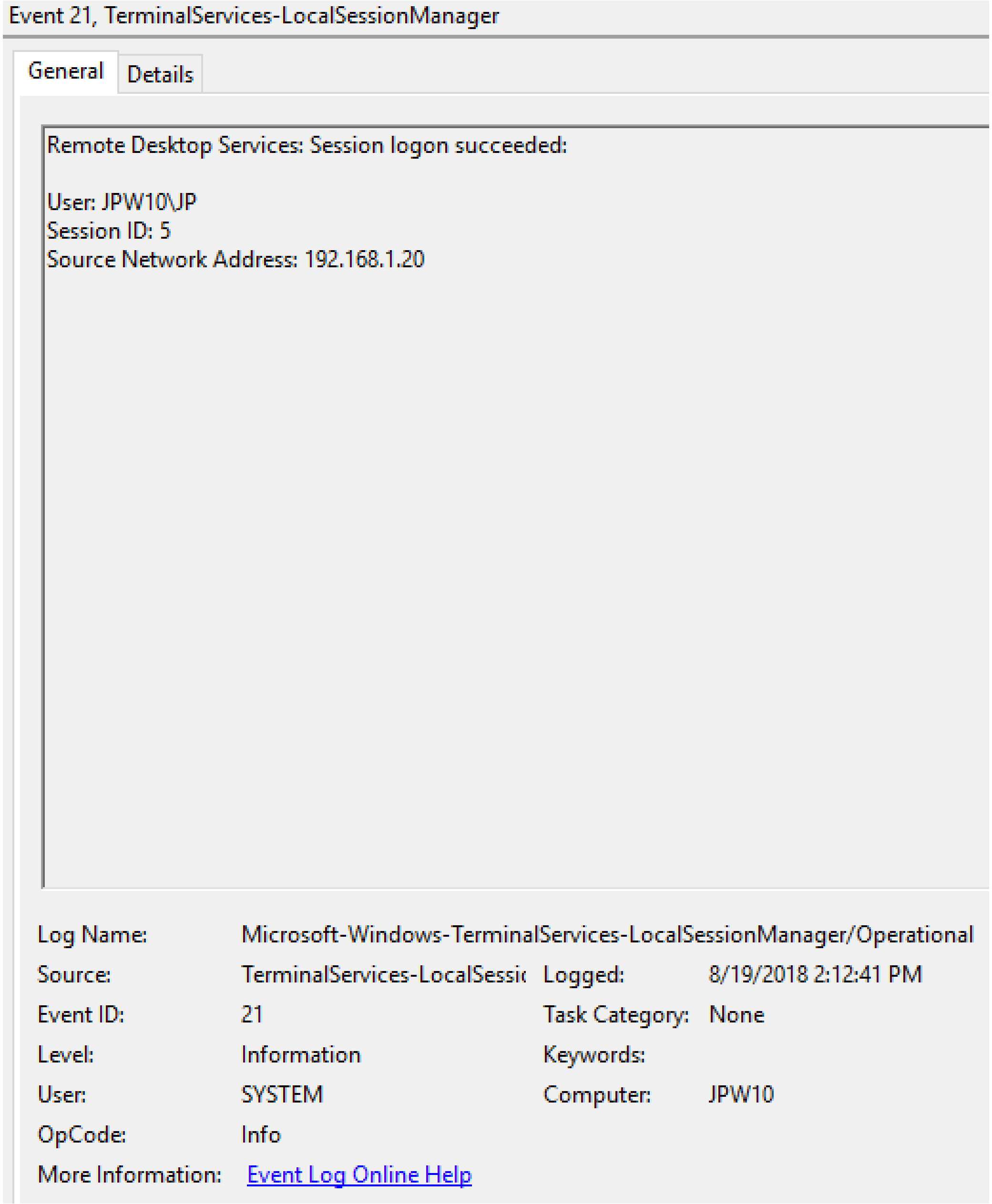
This section covers the ensuing (post-authentication) events that occur upon successful authentication and logon to the system.

Log: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Log Location: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID: 21
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: "Remote Desktop Services: Session logon succeeded:"
Notes: This typically immediately precedes an Event ID 22 when the "Source Network Address" contains a remote IP address. Note that a "Source Network Address" of "LOCAL" simply indicates a local logon and *does NOT* indicate a remote RDP logon. this event with a "Source Network Address" of "LOCAL" will also be generated upon system (re)boot/initialization (shortly before the proceeding associated Event ID 22) . For remote RDP logons, take note of the SessionID as a means of tracking/associating additional Event Log activity with this user's RDP session.

TL;DR: Indicates successful RDP logon and session instantiation, so long as the "Source Network Address" ***is NOT*** "LOCAL".

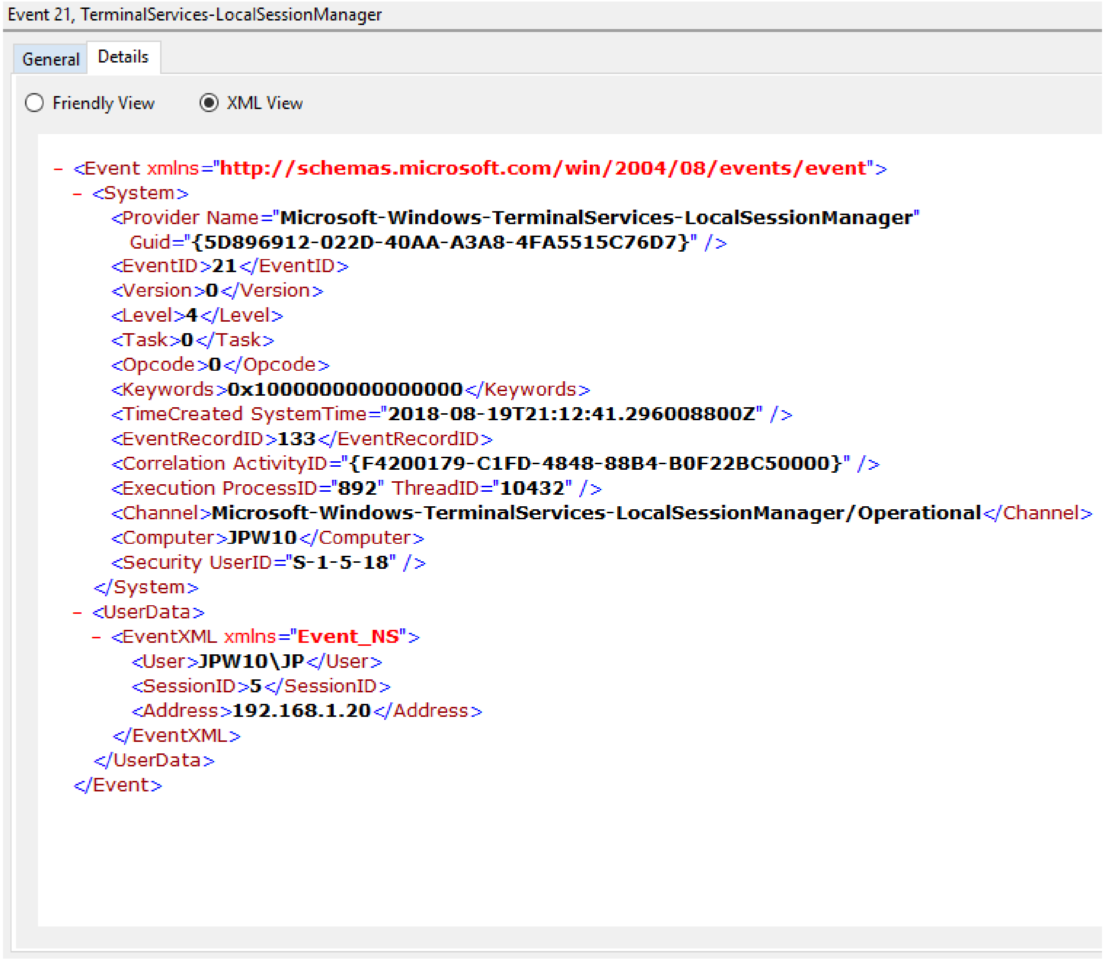


Event 21, TerminalServices-LocalSessionManager

Remote Desktop Services: Session logon succeeded:

User: JPW10\JP
Session ID: 5
Source Network Address: 192.168.1.20

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	8/19/2018 2:12:41 PM
Event ID:	21	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		

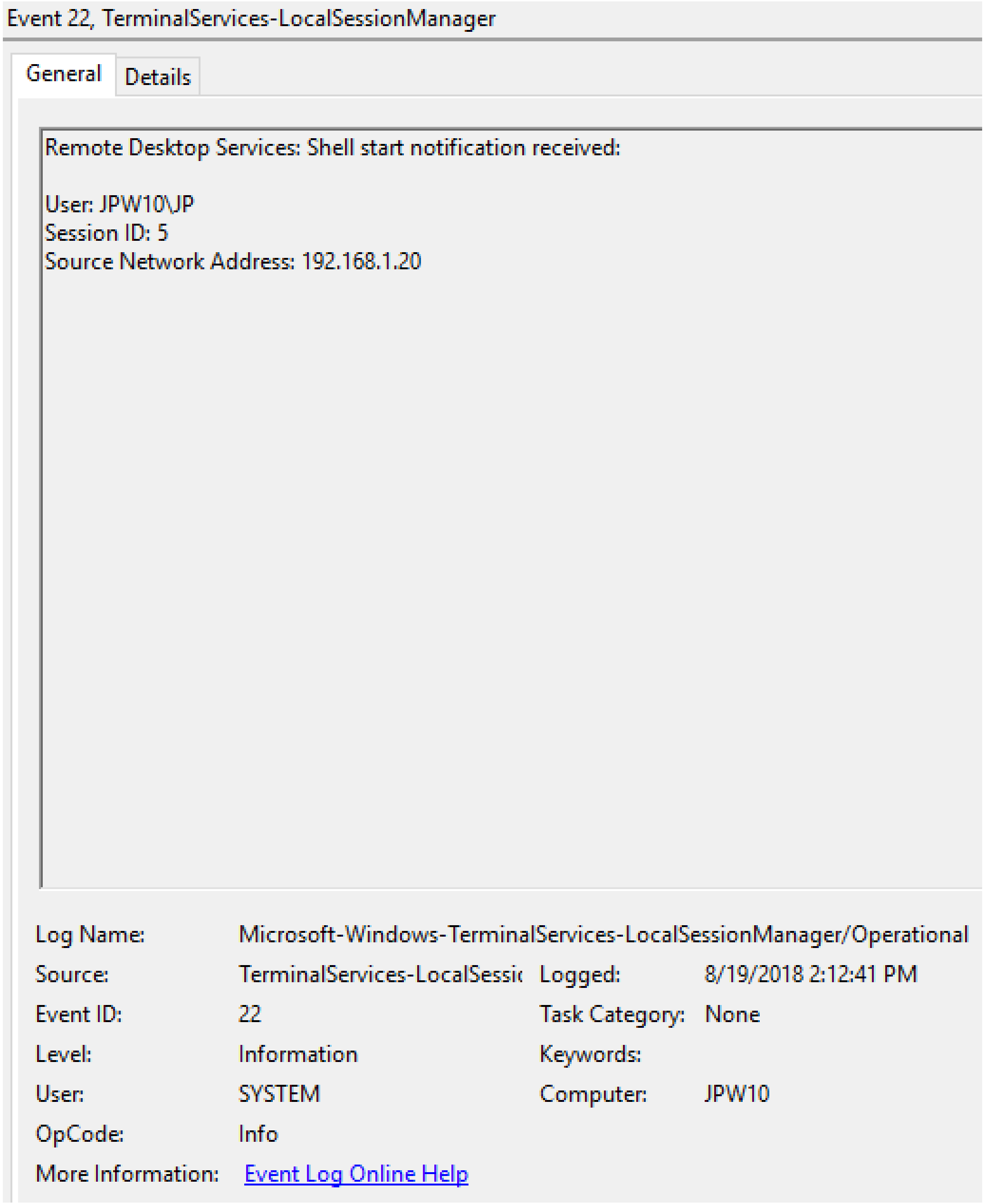


Event 21, TerminalServices-LocalSessionManager

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager"
        Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>21</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-08-19T21:12:41.296008800Z" />
      <EventRecordID>133</EventRecordID>
      <Correlation ActivityID="{F4200179-C1FD-4848-88B4-B0F22BC50000}" />
      <Execution ProcessID="892" ThreadID="10432" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <User>JPW10\JP</User>
        <SessionID>5</SessionID>
        <Address>192.168.1.20</Address>
      </EventXML>
    </UserData>
  </Event>
```

Event ID: 22
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: “Remote Desktop Services: Shell start notification received:”
Notes: This typically immediately proceeds an Event ID 21. Note that a “Source Network Address” of “LOCAL” simply indicates a local logon and *does NOT* indicate a remote RDP logon. This event with a “Source Network Address” of “LOCAL” will also be generated upon system (re)boot/initialization (shortly after the preceding associated Event ID 21).
TL;DR: Indicates successful RDP logon and shell (i.e. Windows GUI Desktop) start, so long as the “Source Network Address” *is NOT* “LOCAL”.

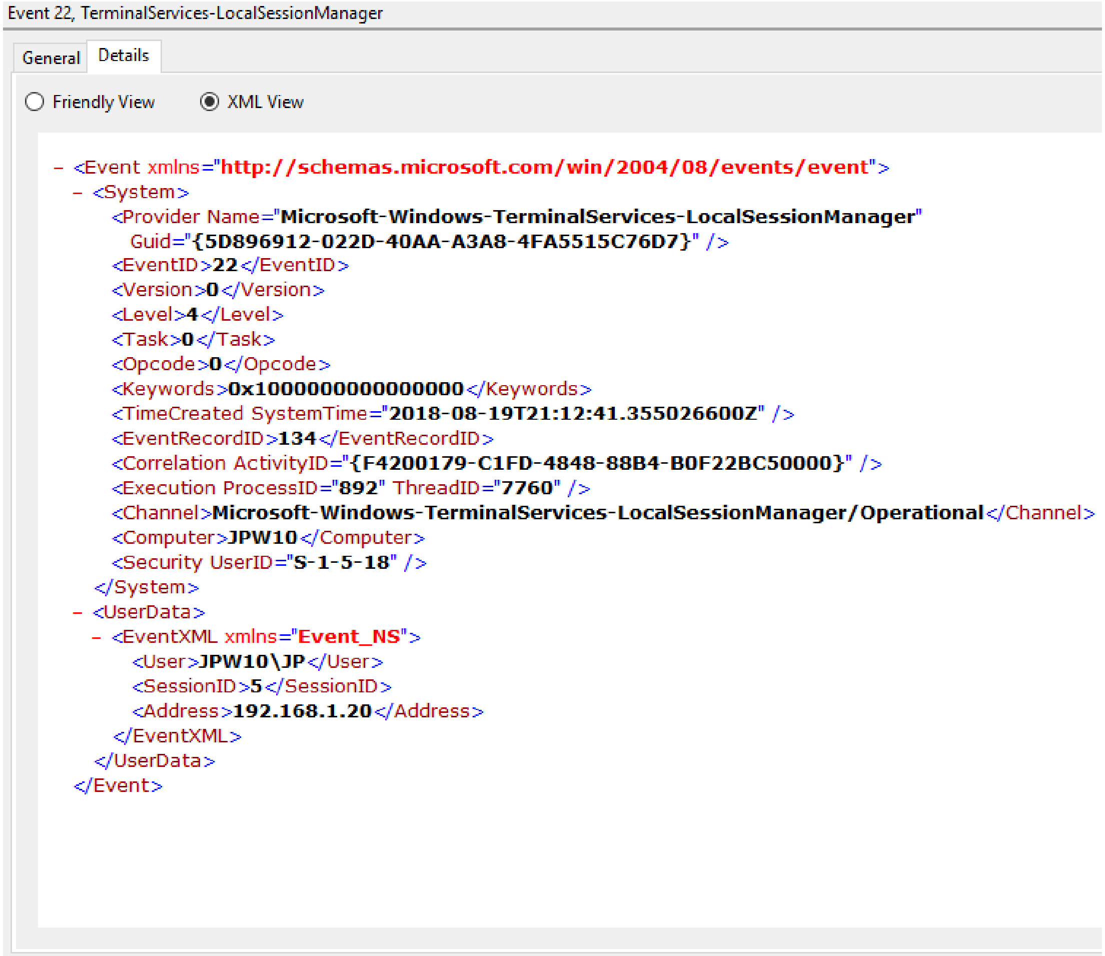


Event 22, TerminalServices-LocalSessionManager

Remote Desktop Services: Shell start notification received:

User: JPW10\JP
Session ID: 5
Source Network Address: 192.168.1.20

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	8/19/2018 2:12:41 PM
Event ID:	22	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		



Event 22, TerminalServices-LocalSessionManager

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager"
        Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>22</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-08-19T21:12:41.355026600Z" />
      <EventRecordID>134</EventRecordID>
      <Correlation ActivityID="{F4200179-C1FD-4848-88B4-B0F22BC50000}" />
      <Execution ProcessID="892" ThreadID="7760" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <User>JPW10\JP</User>
        <SessionID>5</SessionID>
        <Address>192.168.1.20</Address>
      </EventXML>
    </UserData>
  </Event>
```

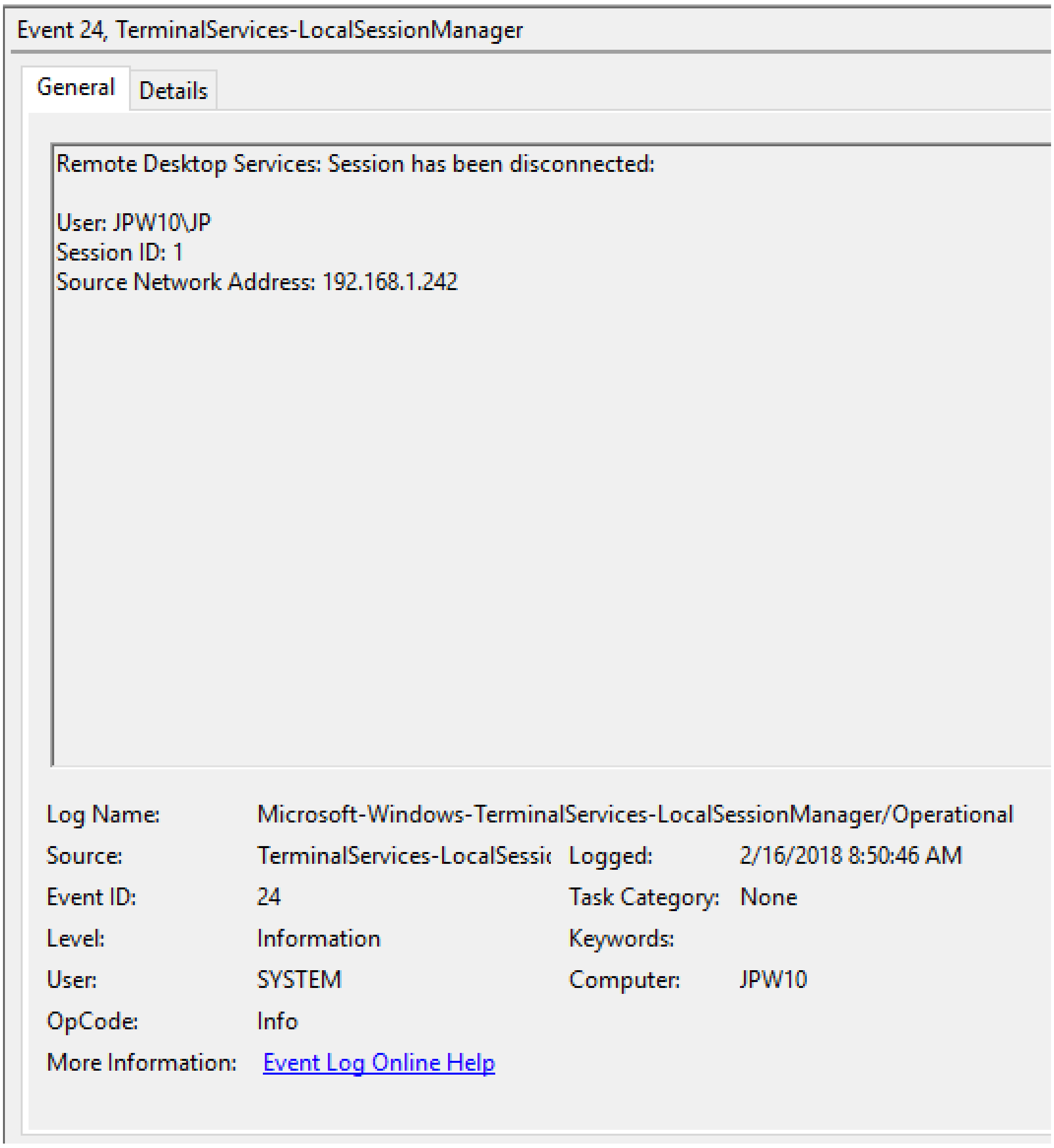
Session Disconnect/Reconnect

This section covers the various session disconnect/reconnect events that might occur due to either system (idle), network (network disconnect), or purposeful user (X out of the RDP window, Start -> Disconnect, Kicked off by another user, etc.) action.

Log: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Log Location: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Event ID: 24
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: "Remote Desktop Services: Session has been disconnected:"
Notes: The user has disconnected from an RDP session, when the "Source Network Address" contains a remote IP address. A "Source Network Address" of "LOCAL" simply indicates a local session disconnection and ***does NOT*** indicate a remote RDP disconnection. Note the "Source Network Address" for the source of the RDP connection. This is typically paired with an Event ID 40. Also take note of the SessionID as a means of tracking/associating additional Event Log activity with this user's RDP session.
TL;DR: The user has disconnected from an RDP session, so long as the "Source Network Address" *is NOT* "LOCAL".

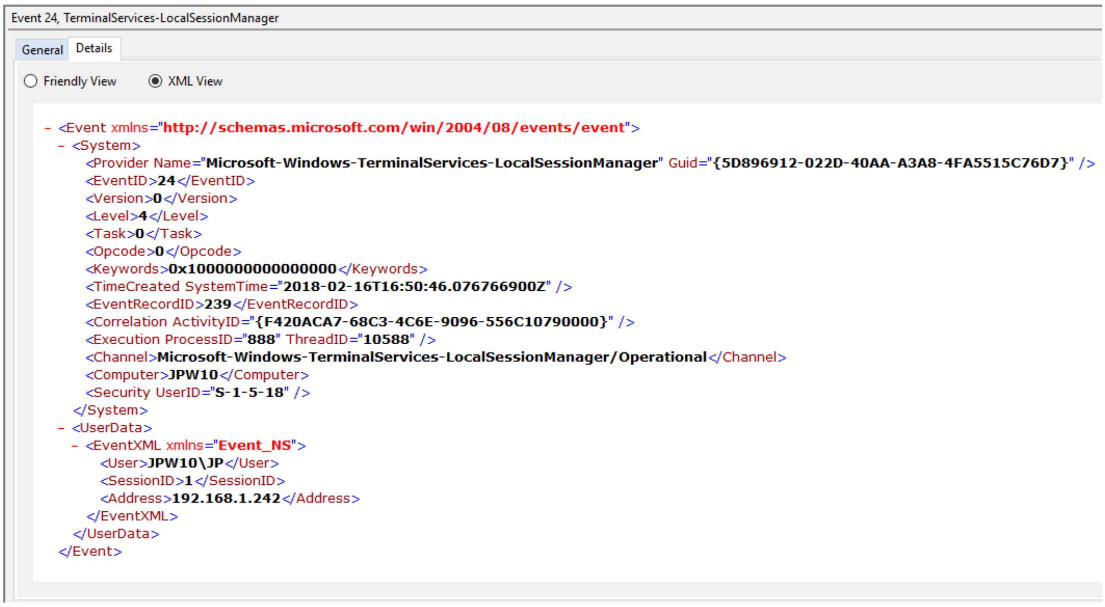


Event 24, TerminalServices-LocalSessionManager

Remote Desktop Services: Session has been disconnected:

User: JPW10\JP
Session ID: 1
Source Network Address: 192.168.1.242

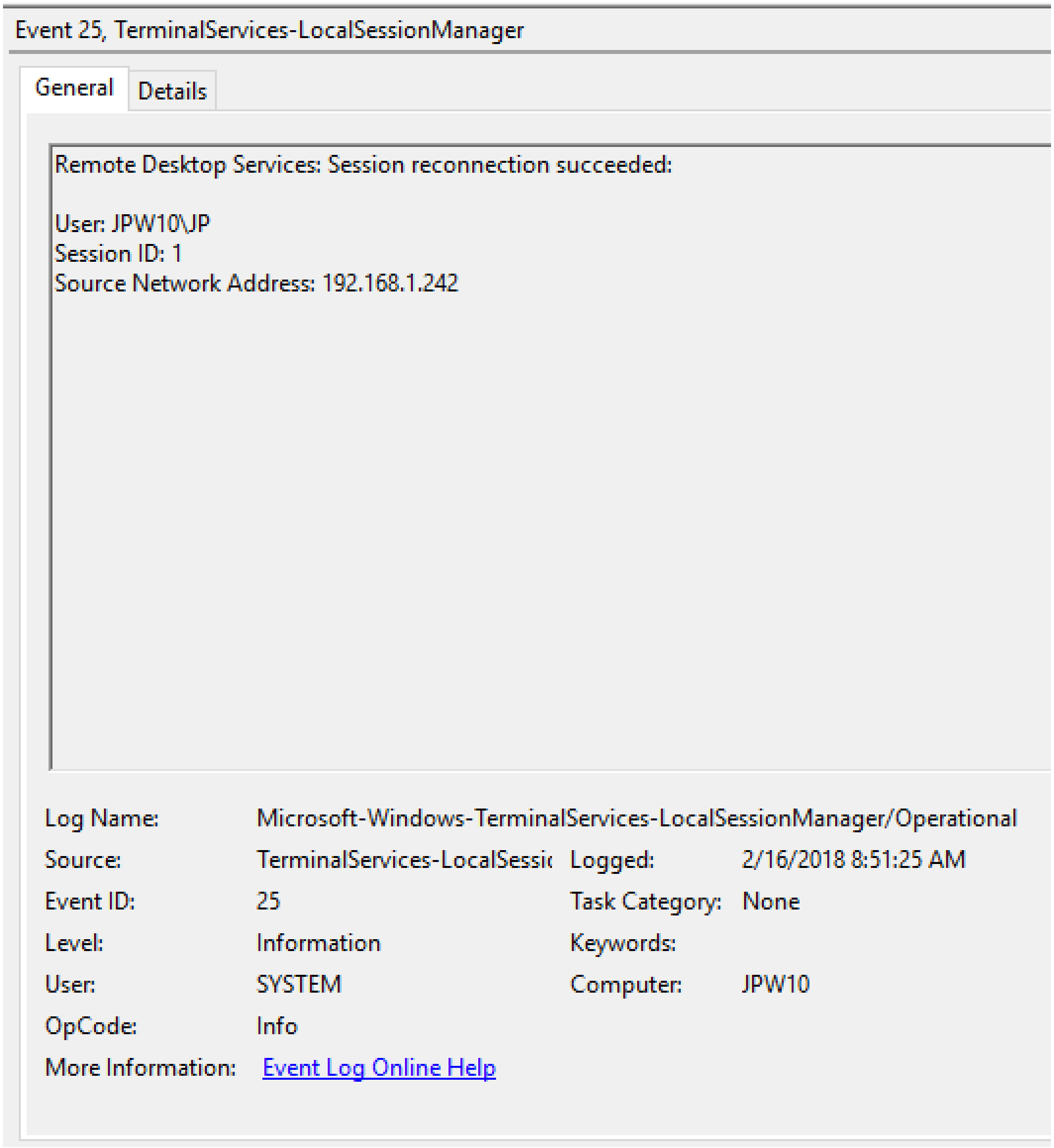
Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	2/16/2018 8:50:46 AM
Event ID:	24	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		



Event 24, TerminalServices-LocalSessionManager

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager" Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>24</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T16:50:46.076766900Z" />
      <EventRecordID>239</EventRecordID>
      <Correlation ActivityID="{F420ACA7-68C3-4C6E-9096-556C10790000}" />
      <Execution ProcessID="888" ThreadID="10588" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <User>JPW10\JP</User>
        <SessionID>1</SessionID>
        <Address>192.168.1.242</Address>
      </EventXML>
    </UserData>
  </Event>
```

Event ID: 25
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: "Remote Desktop Services: Session reconnection succeeded:"
Notes: The user has reconnected to an RDP session, when the "Source Network Address" contains a remote IP address. A "Source Network Address" of "LOCAL" simply indicates a local session reconnection and *does NOT* indicate a remote RDP session reconnection. Note the "Source Network Address" for the source of the RDP connection. This is typically paired with an Event ID 40. Take note of the SessionID as a means of tracking/associating additional Event Log activity with this user's RDP session.
TL;DR: The user has reconnected to an existing RDP session, so long as the "Source Network Address" *is NOT* "LOCAL".

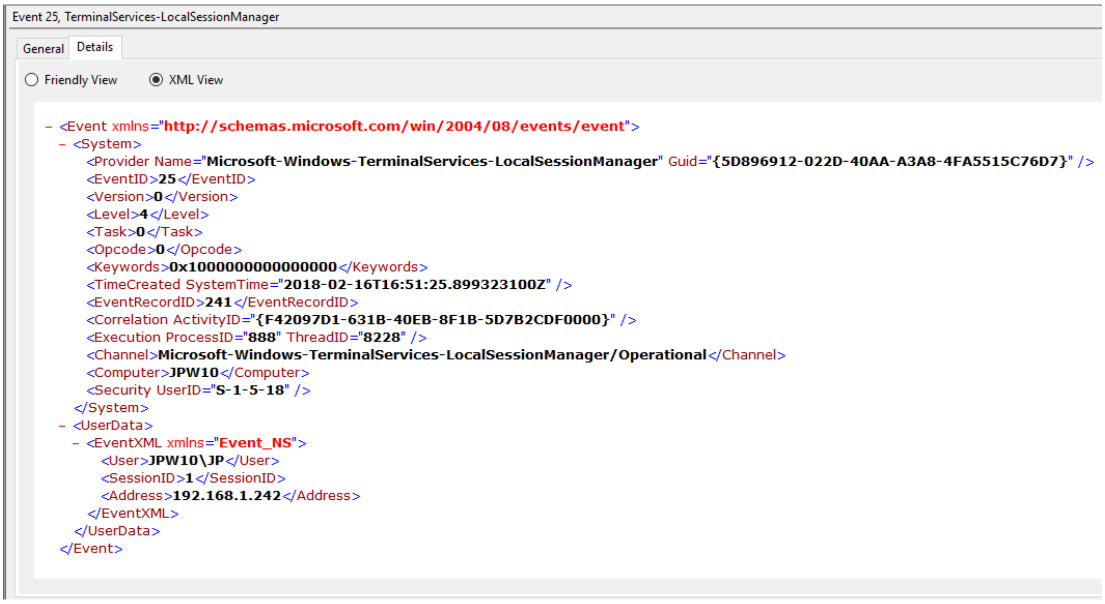


Event 25, TerminalServices-LocalSessionManager

Remote Desktop Services: Session reconnection succeeded:

User: JPW10\JP
Session ID: 1
Source Network Address: 192.168.1.242

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	2/16/2018 8:51:25 AM
Event ID:	25	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		



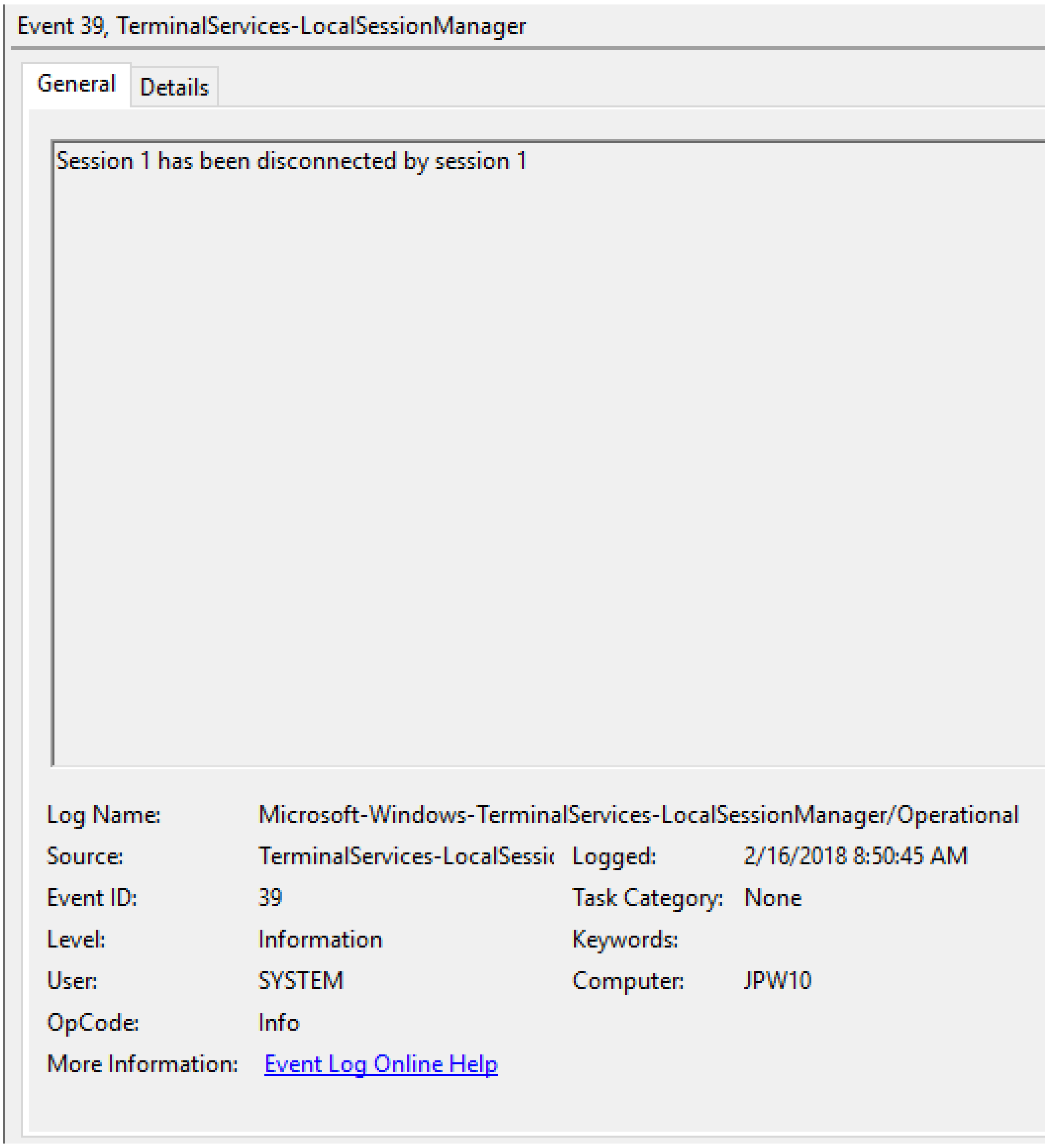
Event 25, TerminalServices-LocalSessionManager

General Details

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager" Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>25</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T16:51:25.899323100Z" />
      <EventRecordID>241</EventRecordID>
      <Correlation ActivityID="{F42097D1-631B-40EB-8F1B-5D7B2CDF0000}" />
      <Execution ProcessID="888" ThreadID="8228" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <User>JPW10\JP</User>
        <SessionID>1</SessionID>
        <Address>192.168.1.242</Address>
      </EventXML>
    </UserData>
  </Event>
```

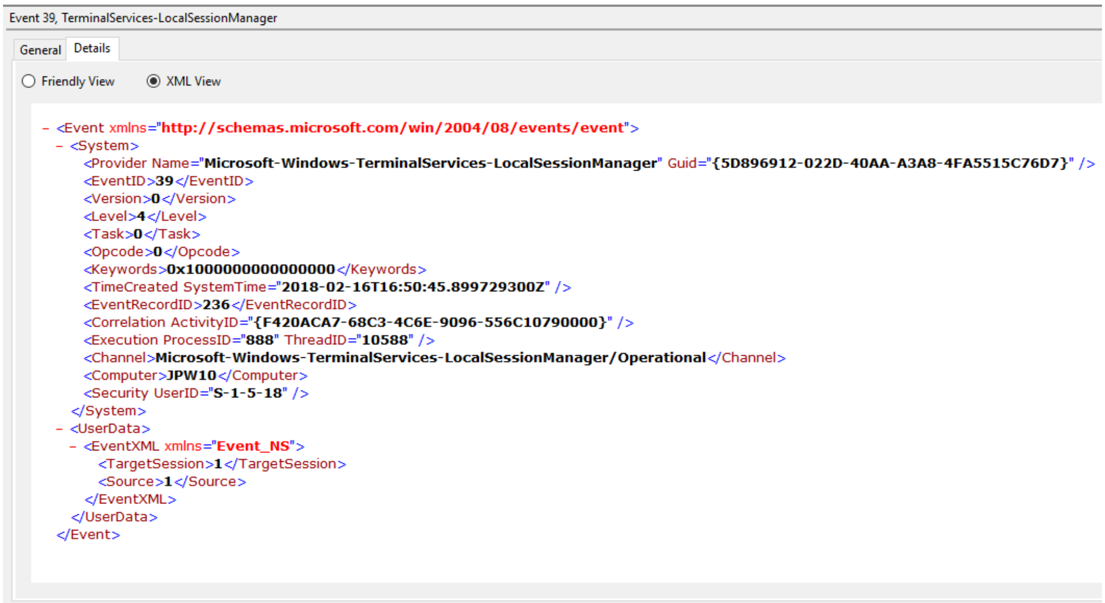
Event ID: 39
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: “Session <X> has been disconnected by session <Y>”
Notes: This indicates that a user has formally disconnected from an RDP session via purposeful Disconnect (e.g., via the Windows Start Menu Disconnect option) versus simply X’ing out of the RDP window. Cases where the Session ID of <X> differs from <Y> may indicate a separate RDP session has disconnected (i.e. kicked off) the given user.
TL;DR: The user formally disconnected from the RDP session.



Event 39, TerminalServices-LocalSessionManager

Session 1 has been disconnected by session 1

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi	Logged:	2/16/2018 8:50:45 AM
Event ID:	39	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		

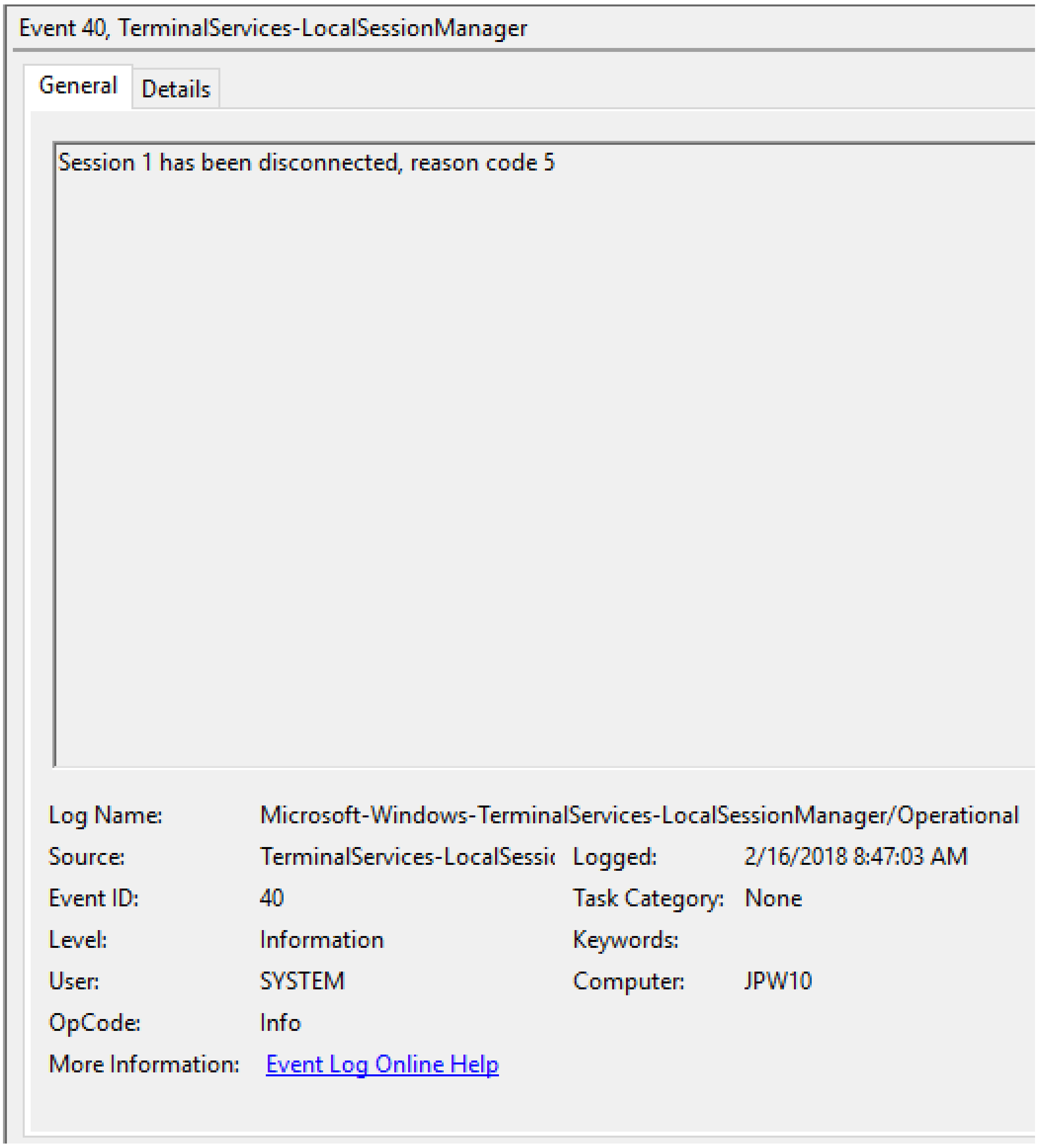


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager" Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>39</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T16:50:45.899729300Z" />
      <EventRecordID>236</EventRecordID>
      <Correlation ActivityID="{F420ACA7-68C3-4C6E-9096-556C10790000}" />
      <Execution ProcessID="888" ThreadID="10588" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <TargetSession>1</TargetSession>
        <Source>1</Source>
      </EventXML>
    </UserData>
  </Event>
```

Event ID: 40
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: “Session <X> has been disconnected, reason code <Z>”
Notes: In true Microsoft fashion, although the description is always “Session has been disconnected”, these events also indicate/correlate to reconnections, not just disconnections. The most helpful information here is the Reason Code (a function of the IMsRdpClient::ExtendedDisconnectReason property), the list of which can be seen here (and this pairs it with the codes to make it easier to read). Below are some examples of codes I encountered during my research.
0 – “No additional information is available.” (Occurs when a user informally X’es out of a session, typically paired with Event ID 24)
5 – “The client’s connection was replaced by another connection.” (Occurs when a user reconnects to an RDP session, typically paired with an Event ID 25)
11 – “User activity has initiated the disconnect.” (Occurs when a user formally initiates an RDP disconnect, for example via the Windows

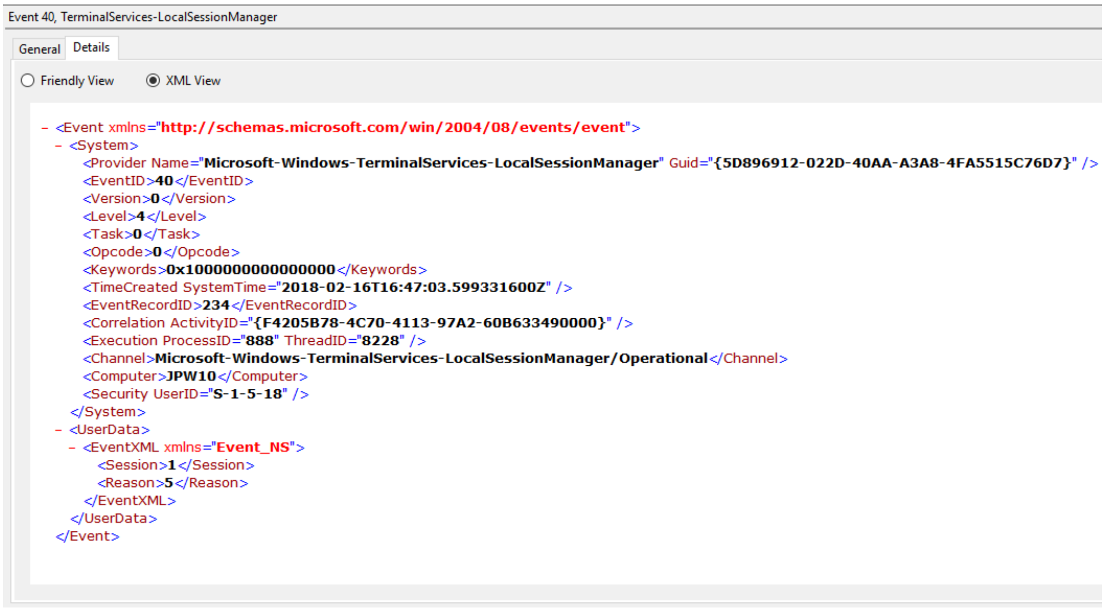
Start Menu Disconnect option.)

TL;DR: The user disconnected from or reconnected to an RDP session.



Session 1 has been disconnected, reason code 5

Log Name: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source: TerminalServices-LocalSessi Logged: 2/16/2018 8:47:03 AM
Event ID: 40 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: JPW10
OpCode: Info
More Information: Event Log Online Help



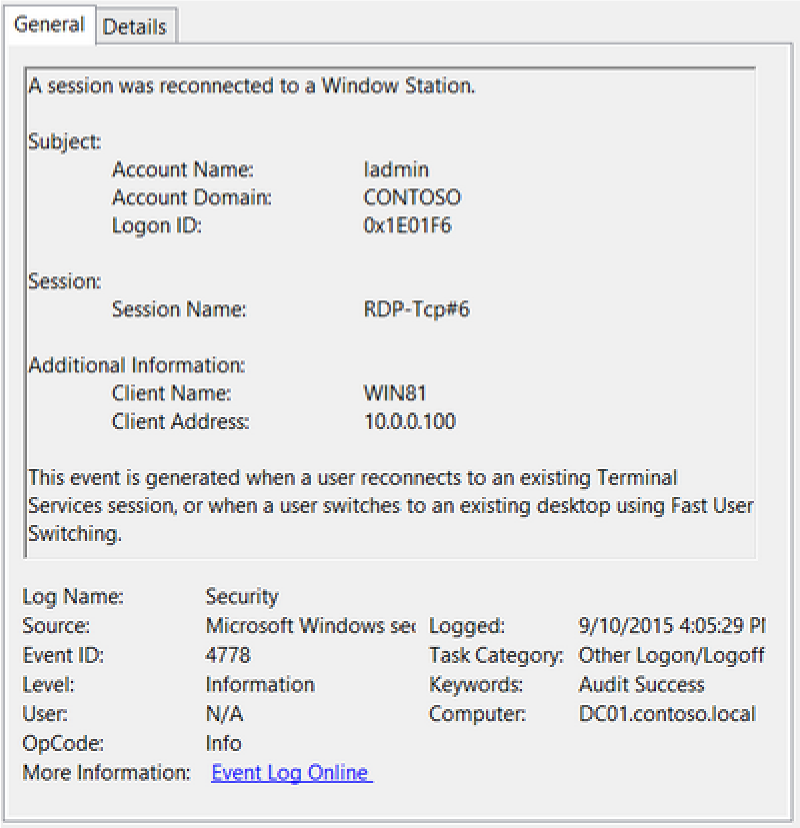
```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager" Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>40</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T16:47:03.599331600Z" />
      <EventRecordID>234</EventRecordID>
      <Correlation ActivityID="{F4205B78-4C70-4113-97A2-60B633490000}" />
      <Execution ProcessID="888" ThreadID="8228" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <Session>1</Session>
        <Reason>5</Reason>
      </EventXML>
    </UserData>
  </Event>
```

Log: Security

Log Location:

%SystemRoot%\System32\Winevt\Logs\Security.evtx

Event ID: 4778
Provider Name: Microsoft-Windows-Security-Auditing
Description: “A session was reconnected to a Window Station.”
Notes: Occurs when a user reconnects to an existing RDP session. Typically paired with Event ID 25. The SessionName, ClientAddress, and LogonID can all be useful for identifying the source and associated activity.
TL;DR: The user reconnected to an existing RDP session.



A session was reconnected to a Window Station.

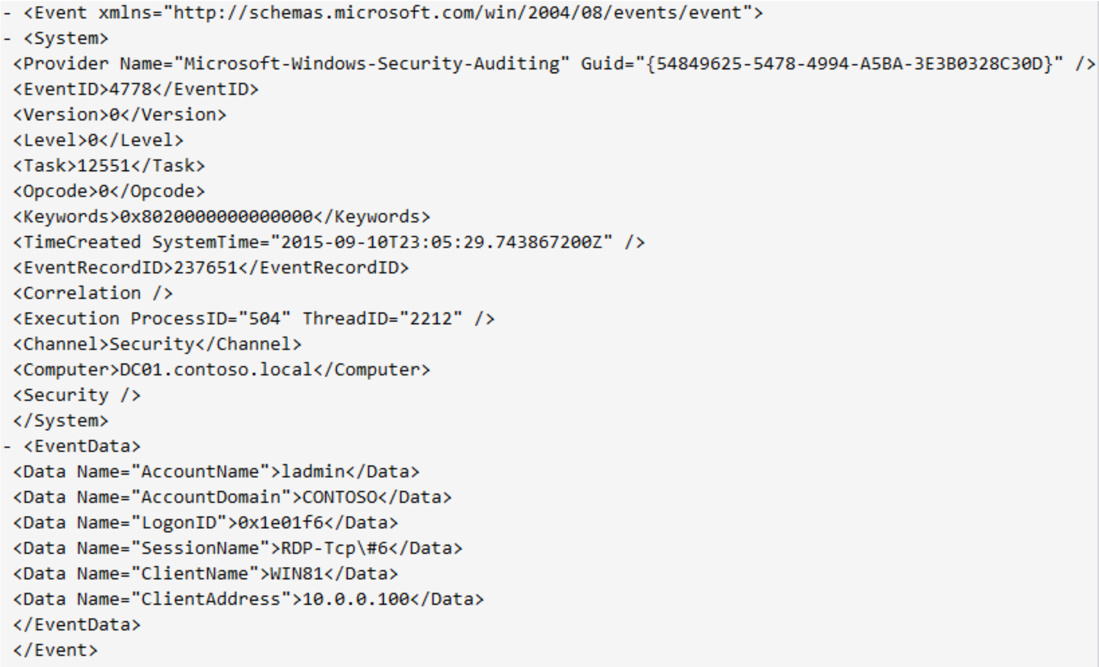
Subject:
    Account Name: ladmin
    Account Domain: CONTOSO
    Logon ID: 0x1E01F6

Session:
    Session Name: RDP-Tcp#6

Additional Information:
    Client Name: WIN81
    Client Address: 10.0.0.100

This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching.

Log Name:	Security		
Source:	Microsoft Windows sec	Logged:	9/10/2015 4:05:29 PI
Event ID:	4778	Task Category:	Other Logon/Logoff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC01.contoso.local
OpCode:	Info		
More Information:	Event Log Online		

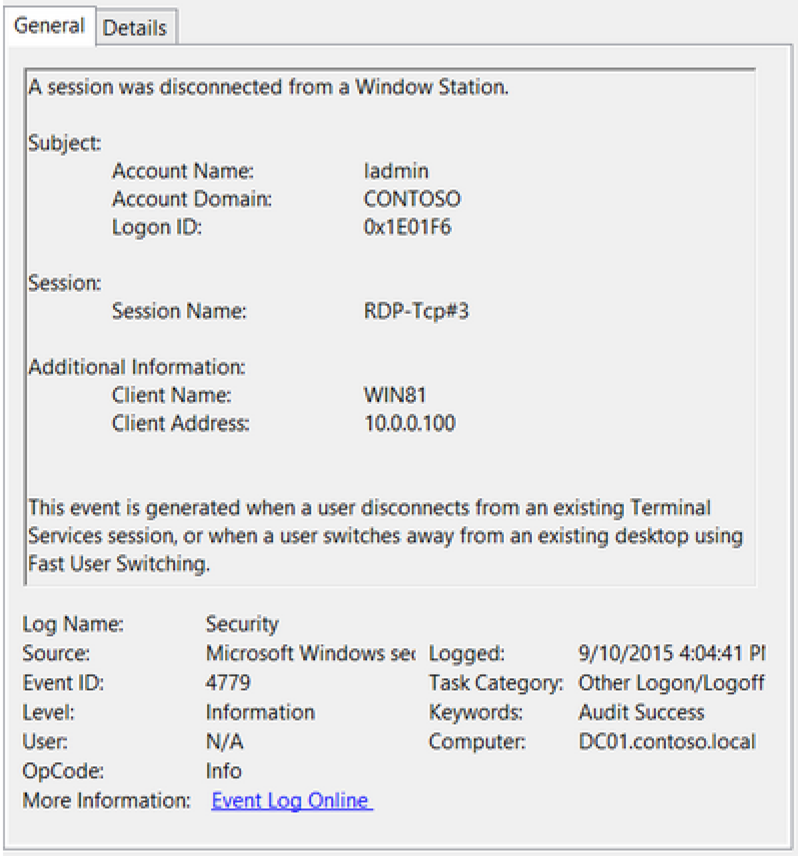


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4778</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12551</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-10T23:05:29.743867200Z" />
 <EventRecordID>237651</EventRecordID>
 <Correlation />
 <Execution ProcessID="504" ThreadID="2212" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="AccountName">ladmin</Data>
 <Data Name="AccountDomain">CONTOSO</Data>
 <Data Name="LogonID">0x1e01f6</Data>
 <Data Name="SessionName">RDP-Tcp\#6</Data>
 <Data Name="ClientName">WIN81</Data>
 <Data Name="ClientAddress">10.0.0.100</Data>
 </EventData>
 </Event>
```

Event ID: 4779

Provider Name: Microsoft-Windows-Security-Auditing

Description: "A session was disconnected from a Window Station."
Notes: Occurs when a user disconnects from an RDP session. Typically paired with Event ID 24 and likely Event ID's 39 and 40. The SessionName, ClientAddress, and LogonID can all be useful for identifying the source and associated activity.
TL;DR: The user disconnected from from an RDP session.



A session was disconnected from a Window Station.

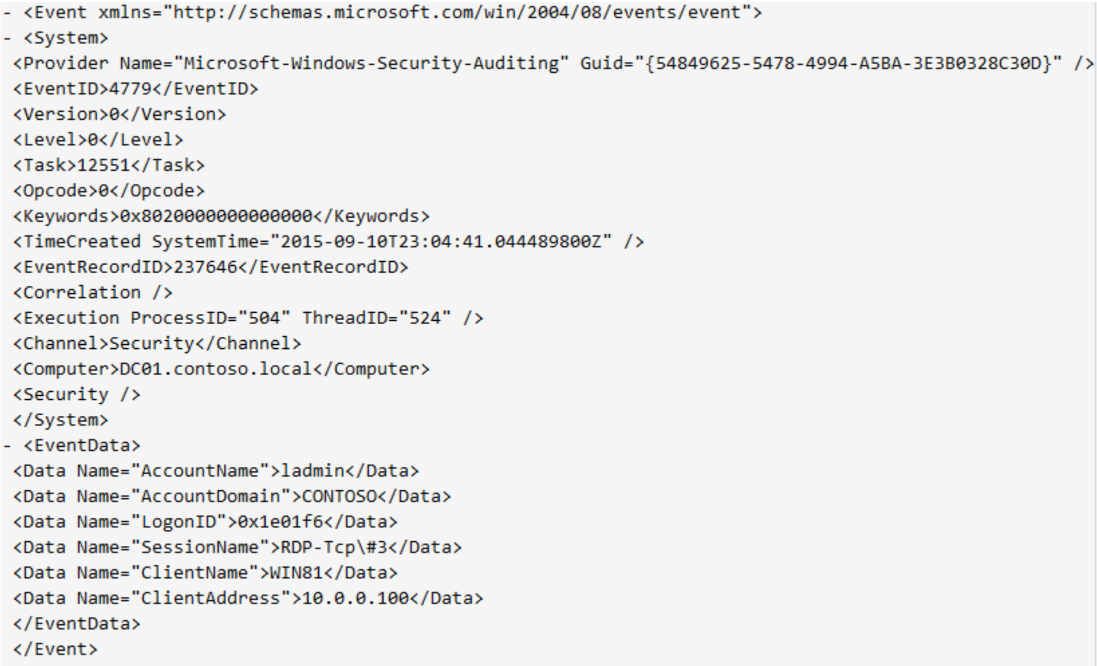
Subject:
    Account Name: ladmin
    Account Domain: CONTOSO
    Logon ID: 0x1E01F6

Session:
    Session Name: RDP-Tcp#3

Additional Information:
    Client Name: WIN81
    Client Address: 10.0.0.100

This event is generated when a user disconnects from an existing Terminal Services session, or when a user switches away from an existing desktop using Fast User Switching.

Log Name:	Security		
Source:	Microsoft Windows sec	Logged:	9/10/2015 4:04:41 PI
Event ID:	4779	Task Category:	Other Logon/Logoff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC01.contoso.local
OpCode:	Info		
More Information:	Event Log Online		



```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4779</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12551</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-10T23:04:41.044489800Z" />
 <EventRecordID>237646</EventRecordID>
 <Correlation />
 <Execution ProcessID="504" ThreadID="524" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="AccountName">ladmin</Data>
 <Data Name="AccountDomain">CONTOSO</Data>
 <Data Name="LogonID">0x1e01f6</Data>
 <Data Name="SessionName">RDP-Tcp\#3</Data>
 <Data Name="ClientName">WIN81</Data>
 <Data Name="ClientAddress">10.0.0.100</Data>
 </EventData>
 </Event>
```

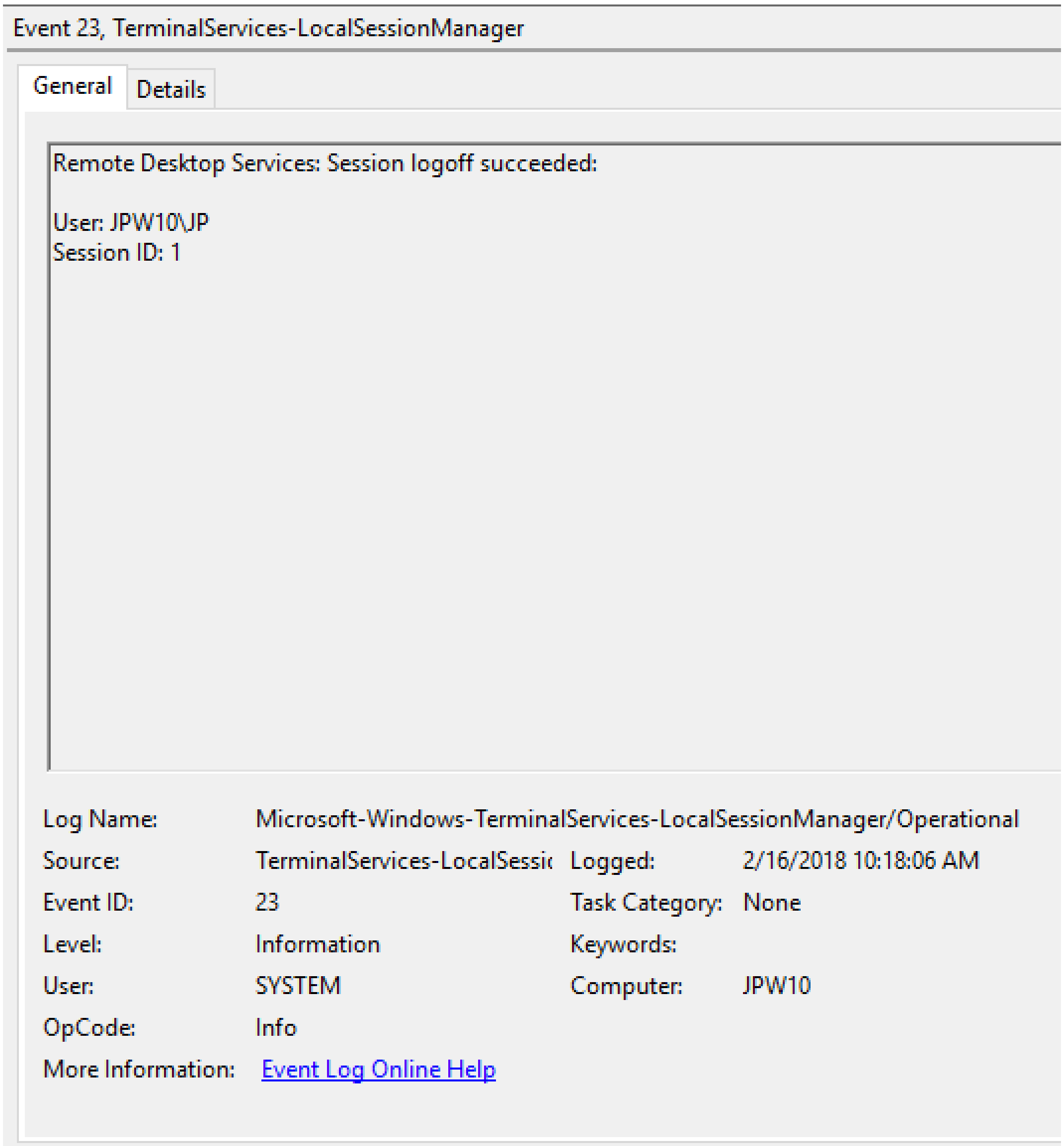
Logoff

This section covers the events that occur after a purposeful (Start -> Disconnect, Start -> Logoff) logoff.

Log: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Log Location: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

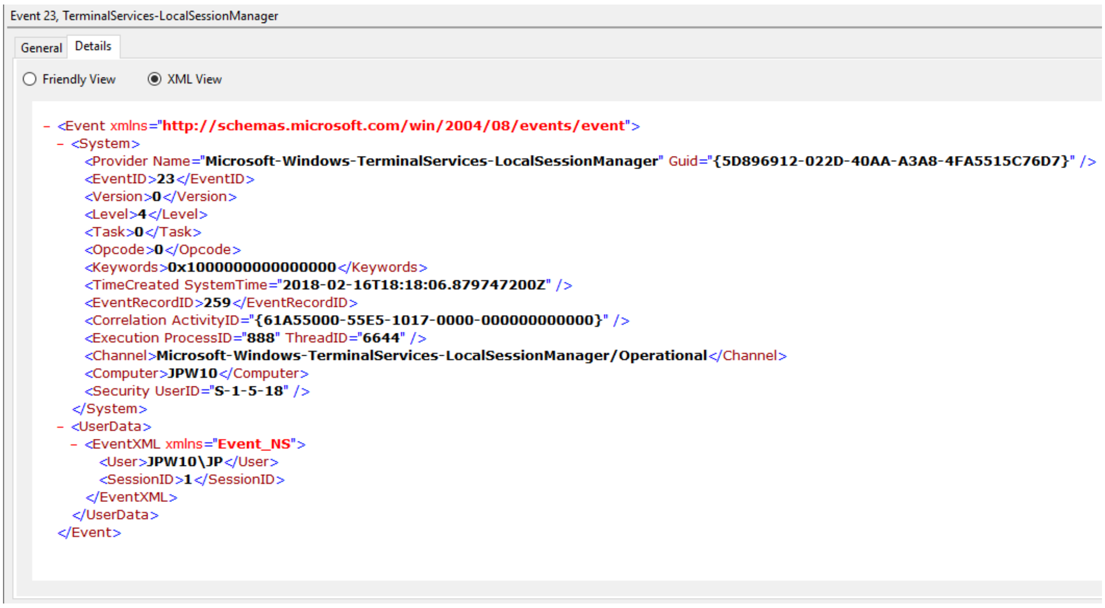
Event ID: 23
Provider Name: Microsoft-Windows-TerminalServices-LocalSessionManager
Description: "Remote Desktop Services: Session logoff succeeded:"
Notes: The user has initiated a logoff. This is typically paired with an Event ID 4634 (logoff). Take note of the SessionID as a means of tracking/associating additional Event Log activity with this user's RDP session. This event with a will also be generated upon a system shutdown/reboot.
TL;DR: The user initiated a formal system logoff (versus a simple session disconnect).



Event 23, TerminalServices-LocalSessionManager

```
Remote Desktop Services: Session logoff succeeded:

User: JPW10\JP
Session ID: 1
```

Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessi(	Logged:	2/16/2018 10:18:06 AM
Event ID:	23	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	JPW10
OpCode:	Info		
More Information:	Event Log Online Help		



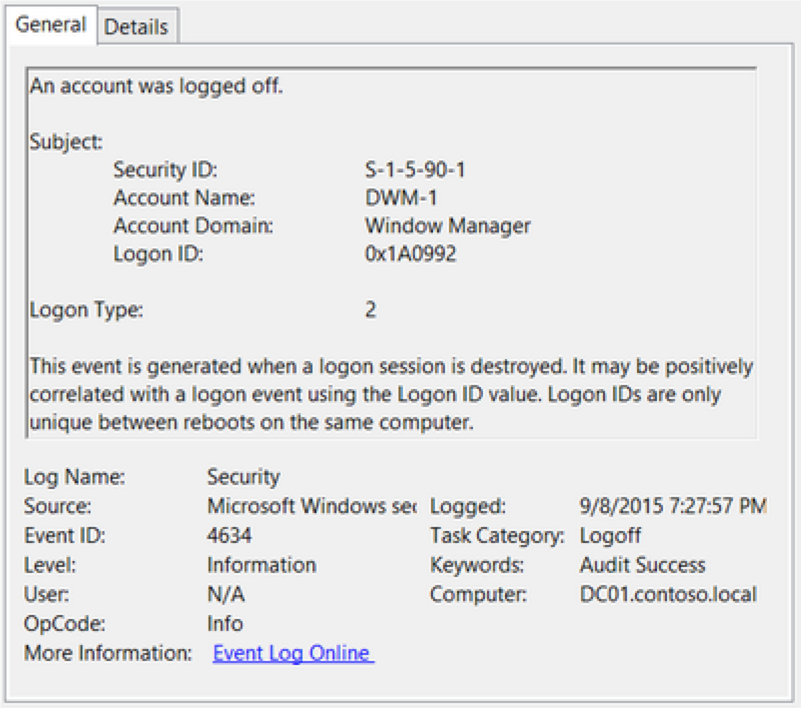
```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-TerminalServices-LocalSessionManager" Guid="{5D896912-022D-40AA-A3A8-4FA5515C76D7}" />
      <EventID>23</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x1000000000000000</Keywords>
      <TimeCreated SystemTime="2018-02-16T18:18:06.879747200Z" />
      <EventRecordID>259</EventRecordID>
      <Correlation ActivityID="{61A55000-55E5-1017-0000-000000000000}" />
      <Execution ProcessID="888" ThreadID="6644" />
      <Channel>Microsoft-Windows-TerminalServices-LocalSessionManager/Operational</Channel>
      <Computer>JPW10</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <EventXML xmlns="Event_NS">
        <User>JPW10\JP</User>
        <SessionID>1</SessionID>
      </EventXML>
    </UserData>
  </Event>
```

Log: Security

Log Location:

%SystemRoot%\System32\Winevt\Logs\Security.evtx

Event ID: 4634
Provider Name: Microsoft-Windows-Security-Auditing
LogonType: 10 (RemoteInteractive / a.k.a. Terminal Services / a.k.a. Remote Desktop) OR Type 7 from a Remote IP (if it's a reconnection from a previous/existing RDP session)
Description: "An account was logged off."
Notes: These occur whenever a user simply disconnects from an RDP session or formally logs off (via Windows Start Menu Logoff). This is typically paired with an Event ID 21 (RDP Session Logoff). I've also discovered these will also be paired (i.e. occur at the same time) with successful authentications (Event ID 4624). Why, I have no idea.
TL;DR: A user disconnected from, or logged off, an RDP session.



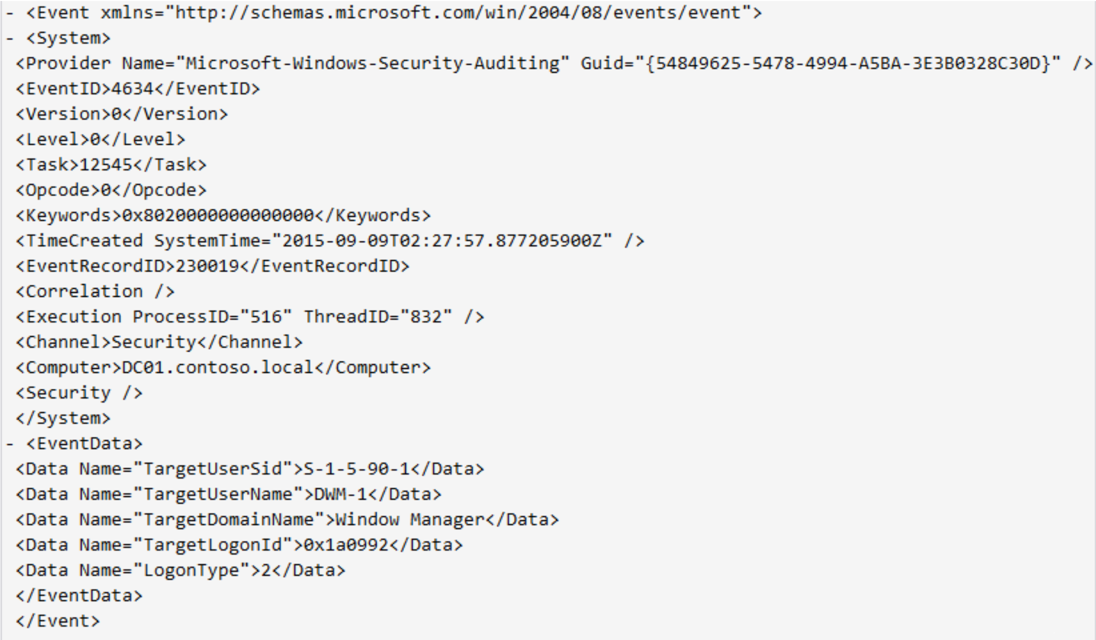
An account was logged off.

Subject:
Security ID: S-1-5-90-1
Account Name: DWM-1
Account Domain: Window Manager
Logon ID: 0x1A0992

Logon Type: 2

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name:	Security		
Source:	Microsoft Windows se	Logged:	9/8/2015 7:27:57 PM
Event ID:	4634	Task Category:	Logoff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC01.contoso.local
OpCode:	Info		
More Information:	Event Log Online		



```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4634</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12545</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-09T02:27:57.877205900Z" />
 <EventRecordID>230019</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="832" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="TargetUserSid">S-1-5-90-1</Data>
 <Data Name="TargetUserName">DWM-1</Data>
 <Data Name="TargetDomainName">Window Manager</Data>
 <Data Name="TargetLogonId">0x1a0992</Data>
 <Data Name="LogonType">2</Data>
 </EventData>
 </Event>
```

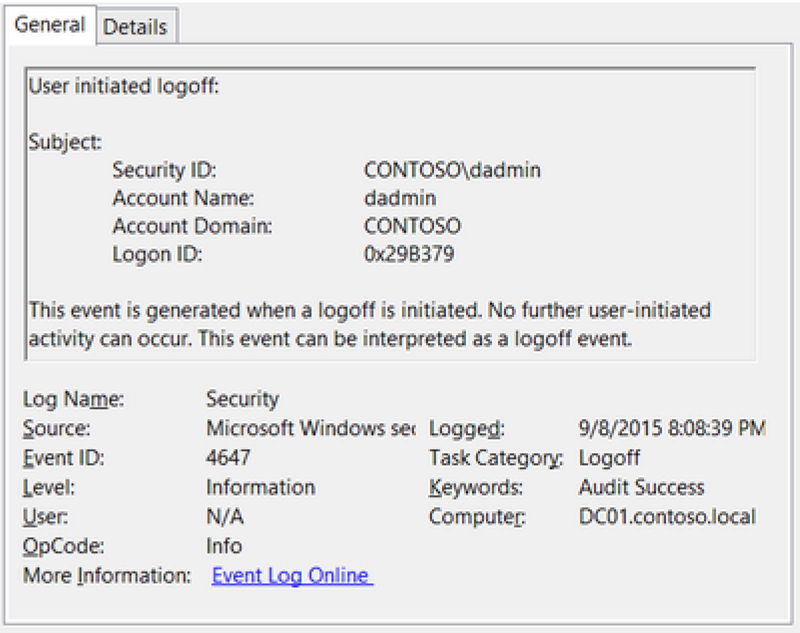
Event ID: 4647

Provider Name: Microsoft-Windows-Security-Auditing

Description: “User initiated logoff:”

Notes: Occurs when a user initiates a formal system logoff and is not necessarily RDP specific. You will need to use some reasoning and temporal analysis to understand if/when it is related to a system logoff via an RDP session or is from a local interactive session as there is no LogonType associated specify which it is.

TL;DR: The user initiated a formal logoff (NOT a simple disconnect).

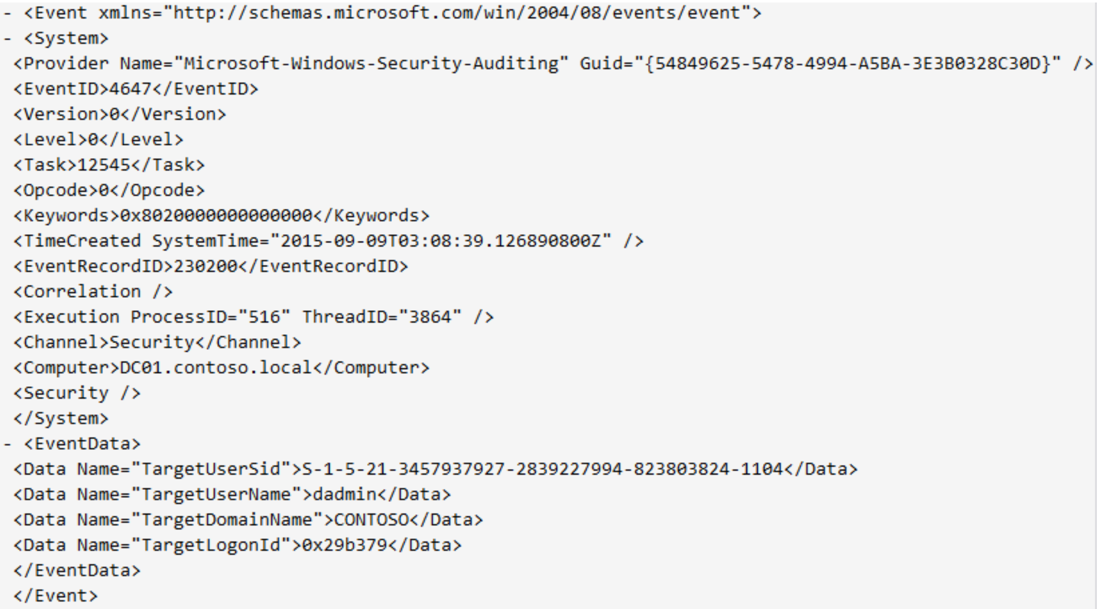


User initiated logoff:

Subject:
Security ID: CONTOSO\dadmin
Account Name: dadmin
Account Domain: CONTOSO
Logon ID: 0x29B379

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.

Log Name: Security
Source: Microsoft Windows sec
Logged: 9/8/2015 8:08:39 PM
Event ID: 4647
Task Category: Logoff
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01.contoso.local
OpCode: Info
More Information: Event Log Online

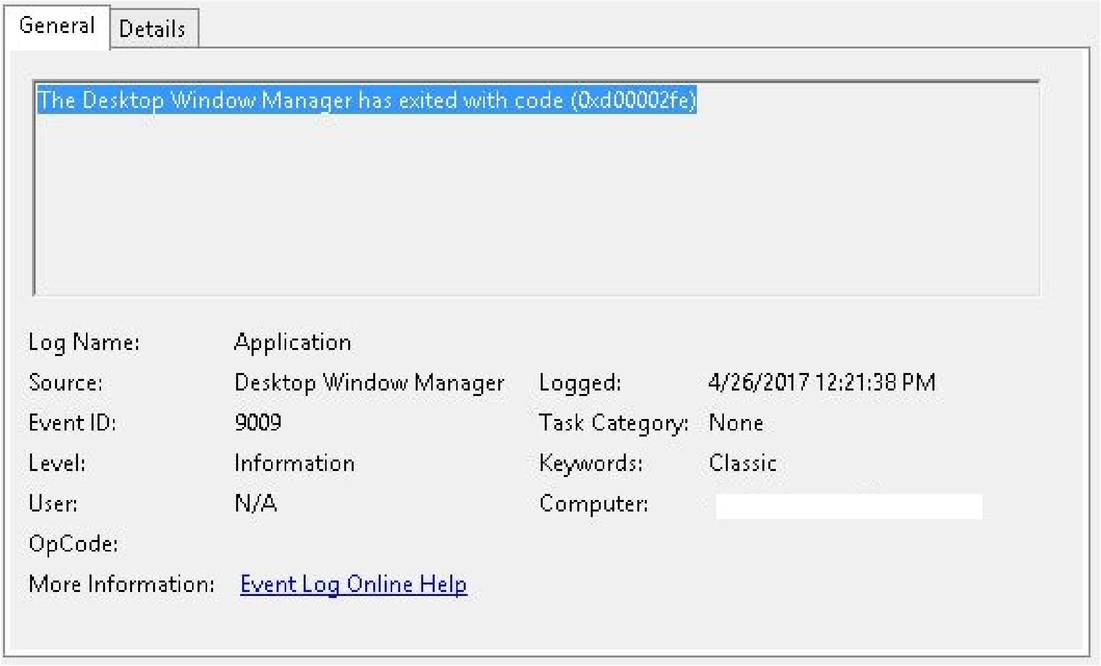


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
 <EventID>4647</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>12545</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-09-09T03:08:39.126890800Z" />
 <EventRecordID>230200</EventRecordID>
 <Correlation />
 <Execution ProcessID="516" ThreadID="3864" />
 <Channel>Security</Channel>
 <Computer>DC01.contoso.local</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="TargetUserSid">S-1-5-21-3457937927-2839227994-823803824-1104</Data>
 <Data Name="TargetUserName">dadmin</Data>
 <Data Name="TargetDomainName">CONTOSO</Data>
 <Data Name="TargetLogonId">0x29b379</Data>
 </EventData>
 </Event>
```

Log: System

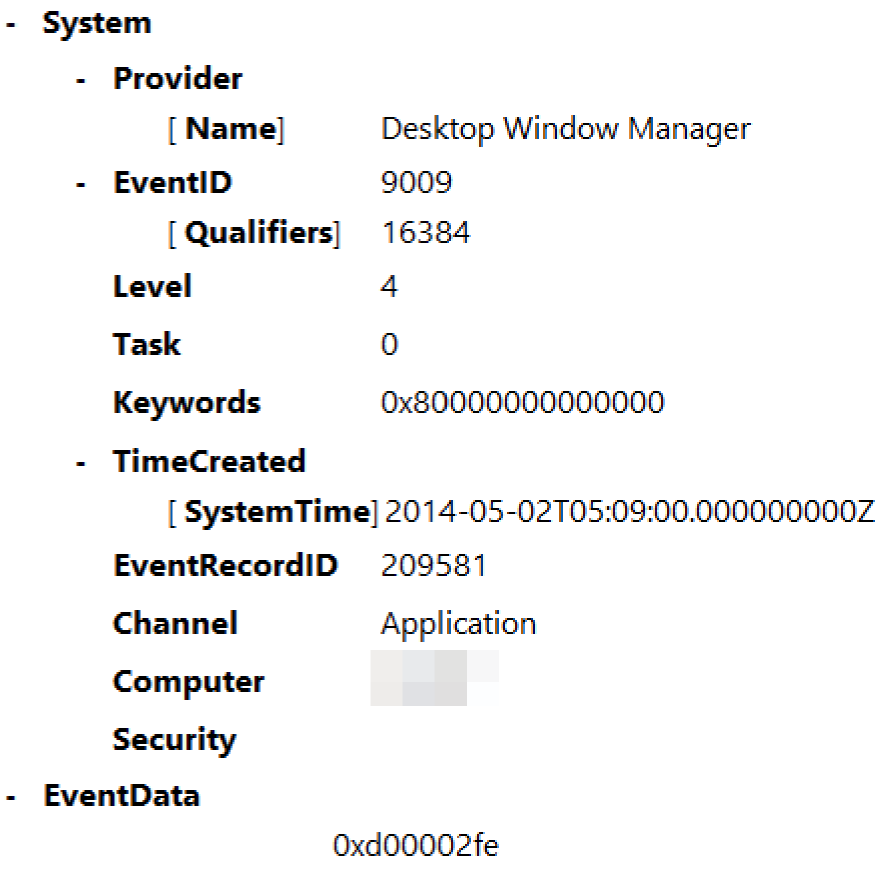
Log Location:
%SystemRoot%\System32\Winevt\Logs\System.evtx

Event ID: 9009
Provider Name: Desktop Window Manager
Description: “The Desktop Window Manager has exited with code (<X>).”
Notes: Occurs when a user formally closes an RDP connection and indicates the RDP desktop GUI has been shut down as a result. This is useful to identify a closed/finalized RDP connection. Though, this event is not always produced for reasons I do not know.
TL;DR: A user has closed out an RDP connection.



The Desktop Window Manager has exited with code (0xd00002fe)

Log Name:	Application		
Source:	Desktop Window Manager	Logged:	4/26/2017 12:21:38 PM
Event ID:	9009	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	[redacted]
OpCode:			
More Information:	Event Log Online Help		



```
- System
    - Provider
          [ Name]        Desktop Window Manager
    - EventID            9009
          [ Qualifiers]  16384
      Level              4
      Task               0
      Keywords           0x80000000000000
    - TimeCreated
          [ SystemTime] 2014-05-02T05:09:00.000000000Z
      EventRecordID      209581
      Channel            Application
      Computer           [redacted]
      Security
- EventData
                      0xd00002fe
```

Wrap-Up

Hopefully that provides a little better insight into some of the most common and (IME) most empirically useful RDP-related Event logs, when/where you might encounter them, what they mean, what they look like, and (most importantly) how they all fit together.

As a result of this post, Richard Davis (@richarddavisg, @13CubedDFIR) of 13Cubed on YouTube has also put together an RDP flow chart that is very helpful in visualizing the expected (though, not guaranteed) flow of these logs. Feel free to check out his short video walkthrough as well.

PREVIOUS

Generating File System Listings from the Command Line (with Full MACB Timestamps and Hashes)

54 Comments

ADD COMMENT →

RDP

Thank you for putting the effort into this and sharing with the community. Only one ask. When doing an RDP from the source as windows to the destination, please also add, to the above, where will the documented log be found, on the source or on the destination.