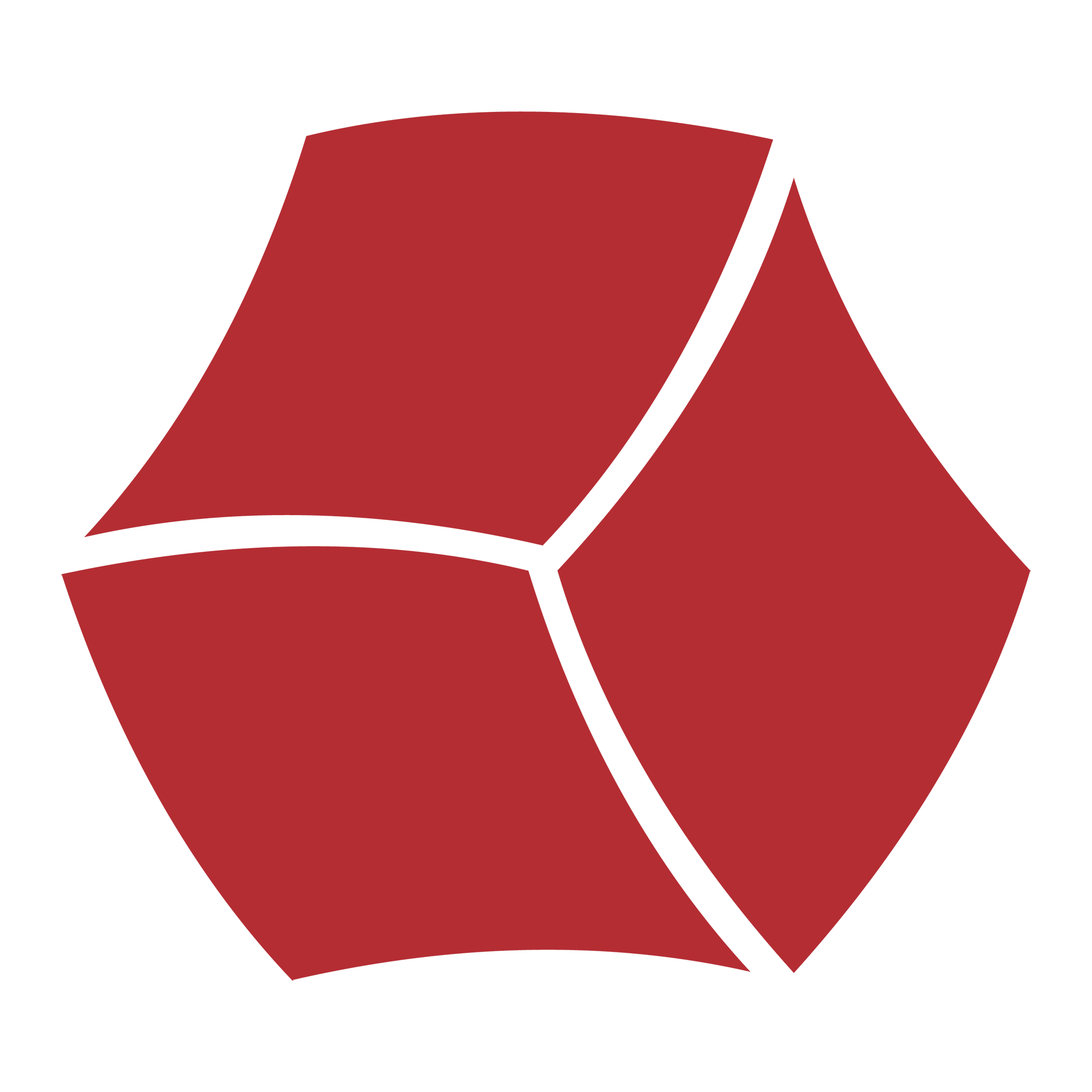
# RDP Successful Logon



Event ID **4624**

Event ID **1149**

Type **10, 7** for Reconnect

Event ID **21** Event ID **22**

*“User authentication succeeded”*

Microsoft-Windows-TerminalServices- RemoteConnectionManager%4Operational.evtx

*“An account was successfully logged on”*

Security.evtx

*“Remote Desktop Services: Session logon succeeded:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“Remote Desktop Services: Shell start notification received:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

### Network Connection Authentication Logon

}

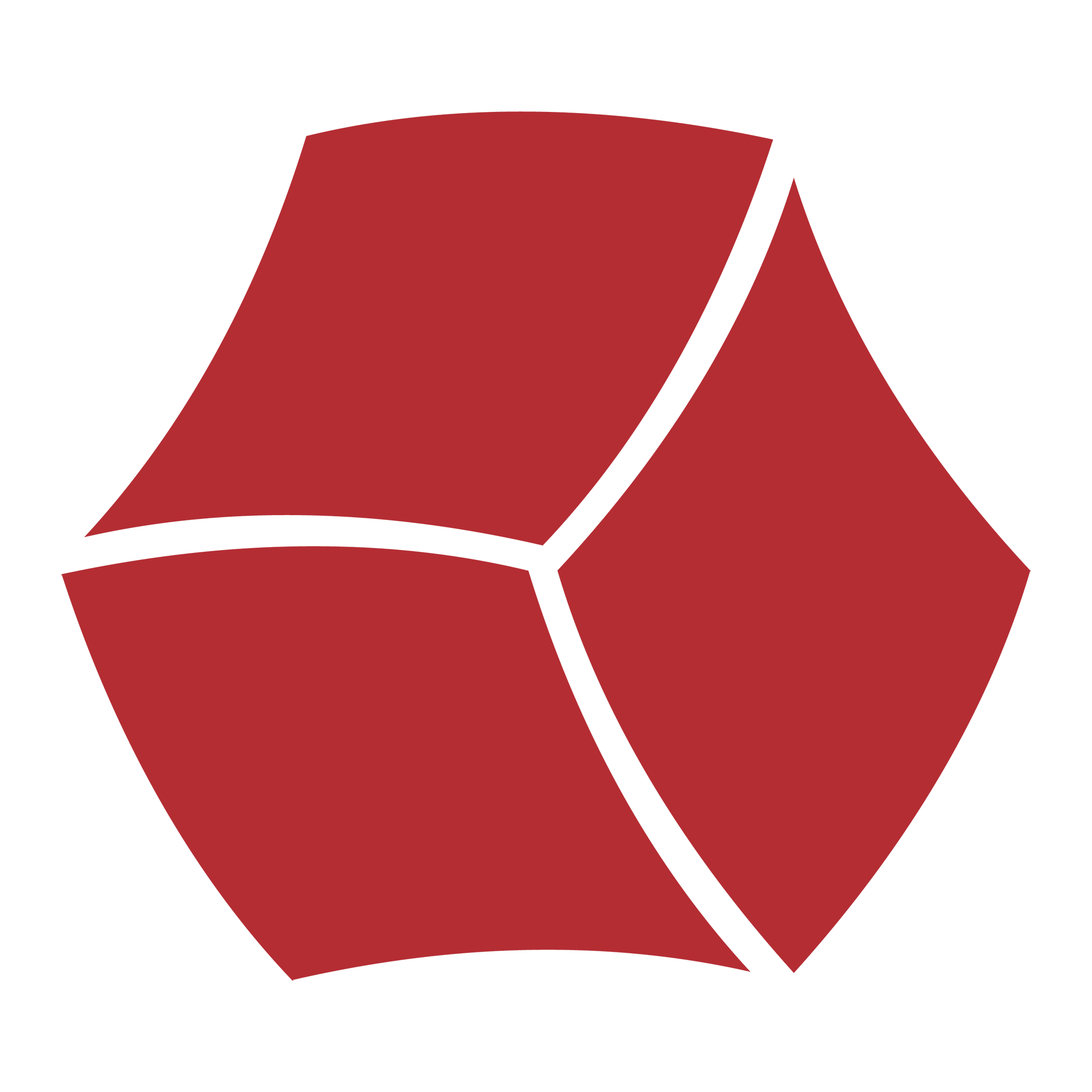
}

}

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed

# RDP Unsuccessful Logon



Event ID **4625**

Event ID **1149**

Type **10, 7** for Reconnect

*“User authentication succeeded”*

Microsoft-Windows-TerminalServices- RemoteConnectionManager%4Operational.evtx

*“An account failed to log on”*

Security.evtx

### Network Connection Authentication

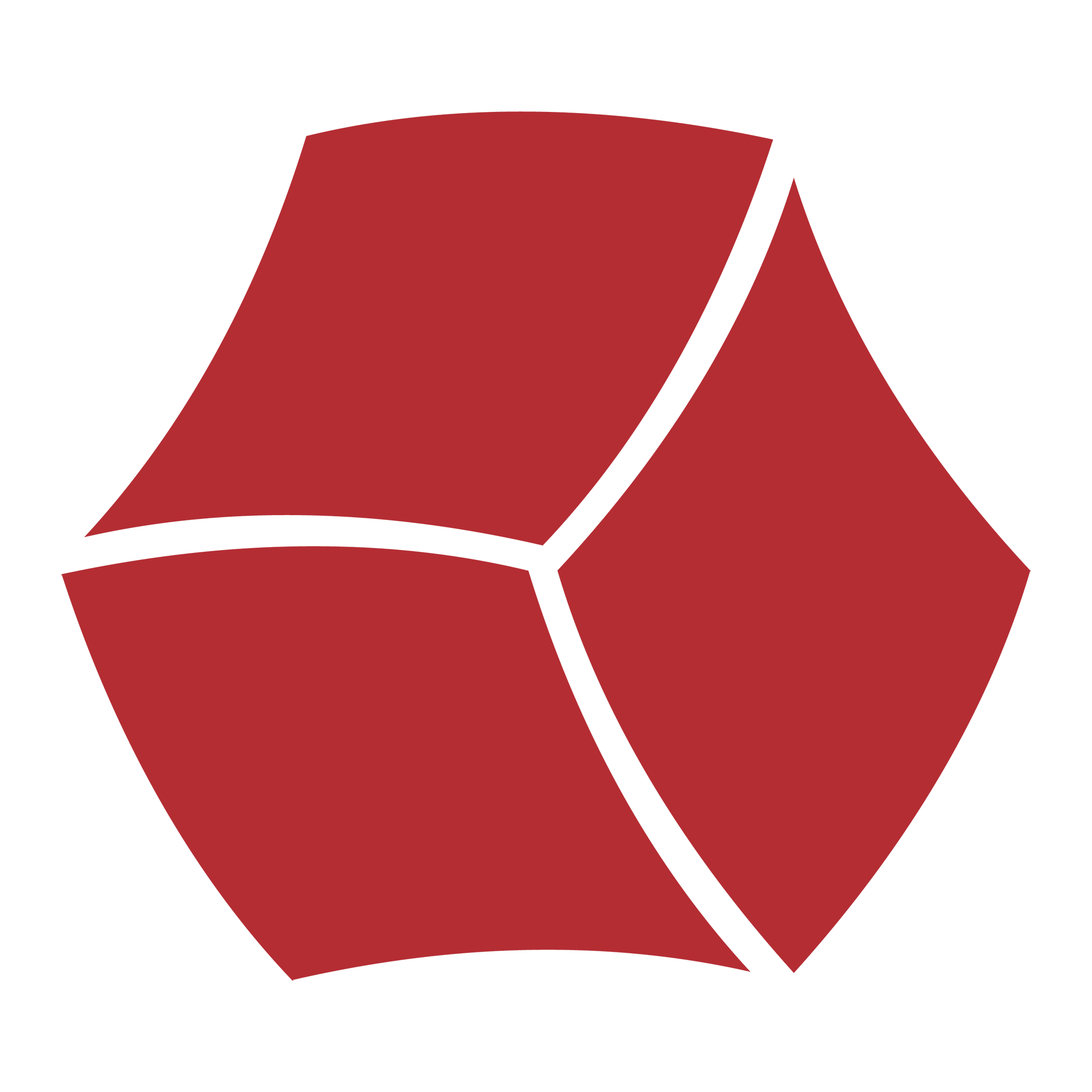
}

}

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed

# RDP Session Disconnect



## (Window Close)

Event ID **24** Event ID **40** Event ID **4779**

Event ID **4634**

Type **10, 7** for Reconnect

*“Remote Desktop Services: Session has been disconnected:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“Session <X> has been disconnected, reason code <Z>”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“A session was disconnected from a Window Station”*

Security.evtx

*“An account was logged oﬀ”*

Security.evtx

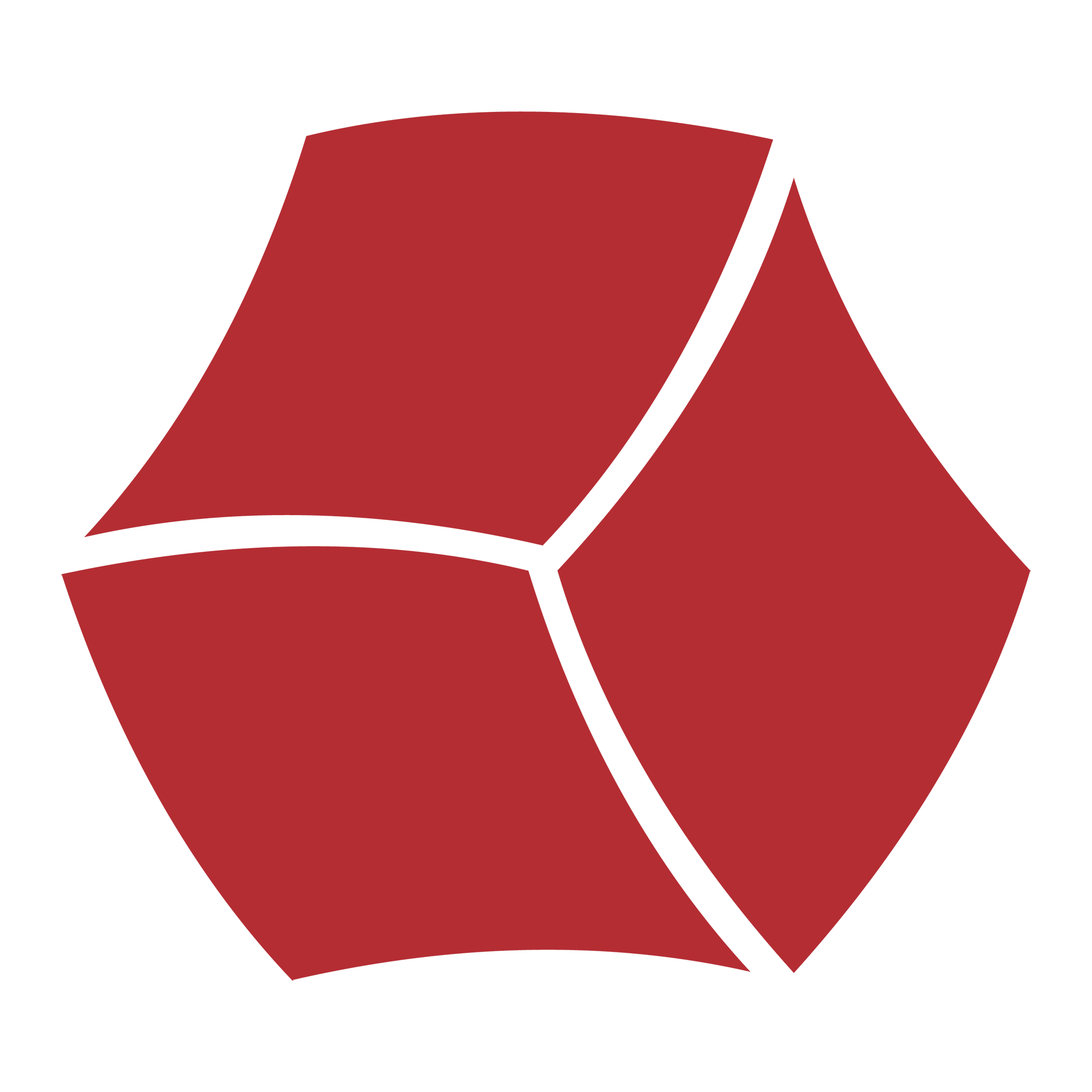
### Session Disconnect / Reconnect

}

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed

# RDP Session Disconnect



## (Purposeful Disconnect via Start > Disconnect)

#### Event ID **24**

#### Event ID **39**

Event ID **40** Event ID **4779**

Event ID **4634**

Type **10, 7** for Reconnect

*“Remote Desktop Services: Session has been disconnected:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“Session <X> has been disconnected by session <Y>”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“Session <X> has been disconnected, reason code <Z>”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“A session was disconnected from a Window Station”*

Security.evtx

*“An account was logged oﬀ”*

Security.evtx

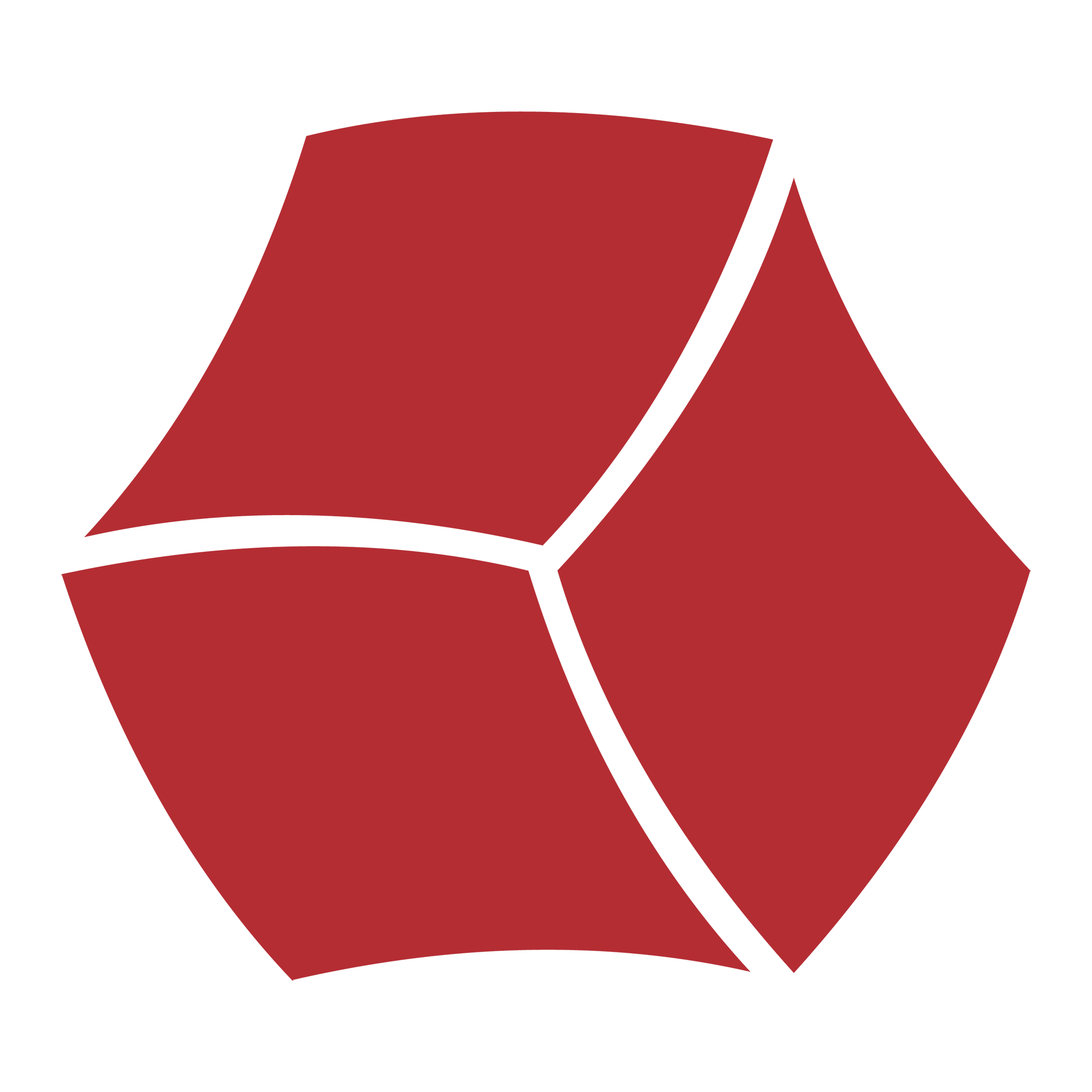
### Session Disconnect / Reconnect

}

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed

# RDP Session Reconnect



Event ID **1149**

Event ID **4624**

Type **7**

#### Event ID **25**

Event ID **40\***

Event ID **4778**

*“User authentication succeeded”*

Microsoft-Windows-TerminalServices- RemoteConnectionManager%4Operational.evtx

*“An account was successfully logged on”*

Security.evtx

*“Remote Desktop Services: Session reconnection succeeded:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“Session <X> has been disconnected, reason code <Z>”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

\*Events also indicate/correlate to reconnections

*“A session was reconnected to a Window Station”*

Security.evtx

**Network Connection**

}

}

}

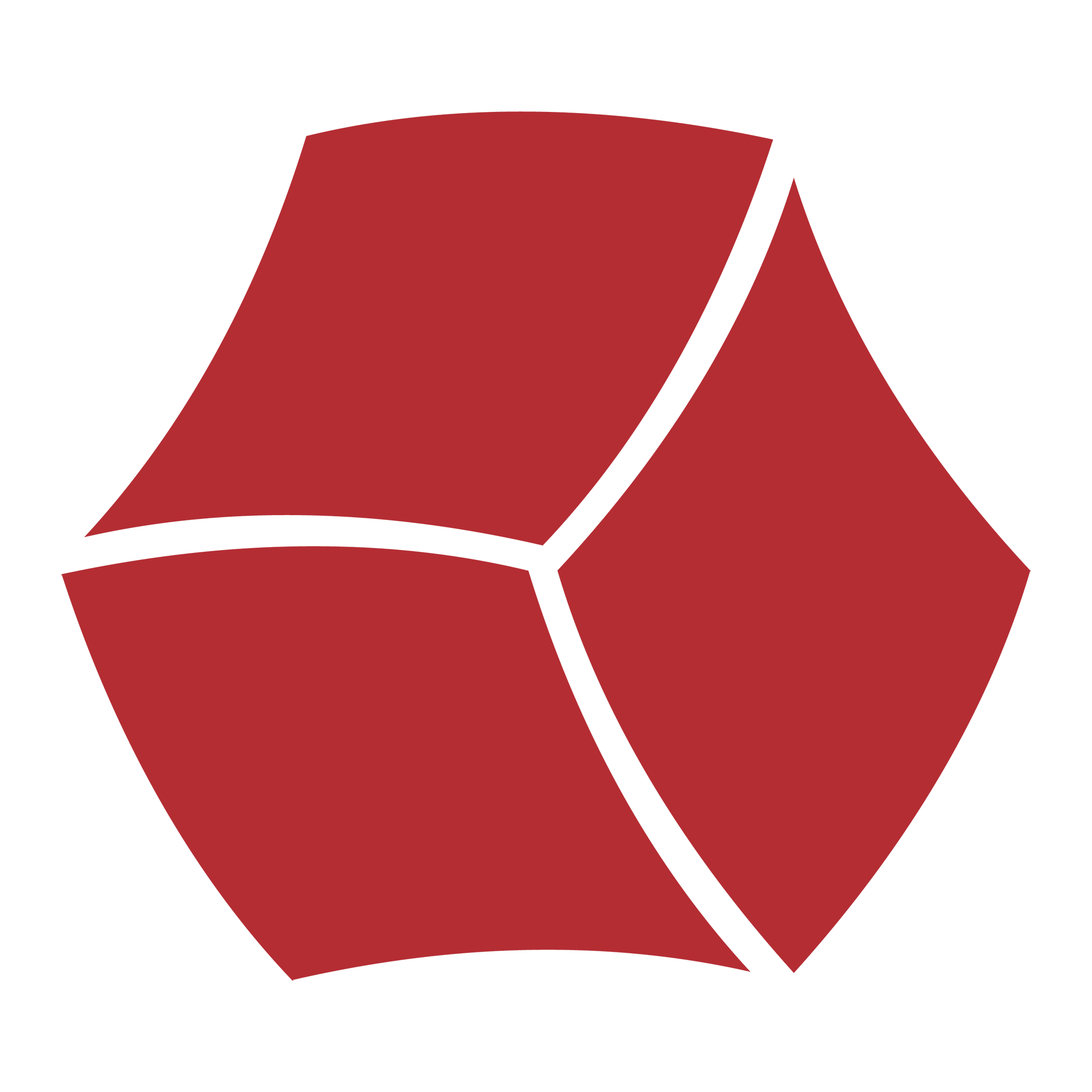
**Authentication**

**Session Disconnect / Reconnect**

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed

# RDP Session Logoff



#### Event ID **23**

Event ID **4634**

Type **10, 7** for Reconnect

Event ID **4647**

Event ID **9009**

*“Remote Desktop Services: Session logoﬀ succeeded:”*

Microsoft-Windows-TerminalServices- LocalSessionManager%4Operational.evtx

*“An account was logged oﬀ”*

Security.evtx

*“User initiated logoﬀ:”*

Security.evtx

*“The Desktop Window Manager has exited with code (<X>).”*

System.evtx

### Logoff

}

Source: https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation

youtube.com/13cubed