Inversion6

Microsoft Quick Assist Forensics

Tyler Hudak

March 2025

B-Sides Rochester

IR Profile: Tyler Hudak

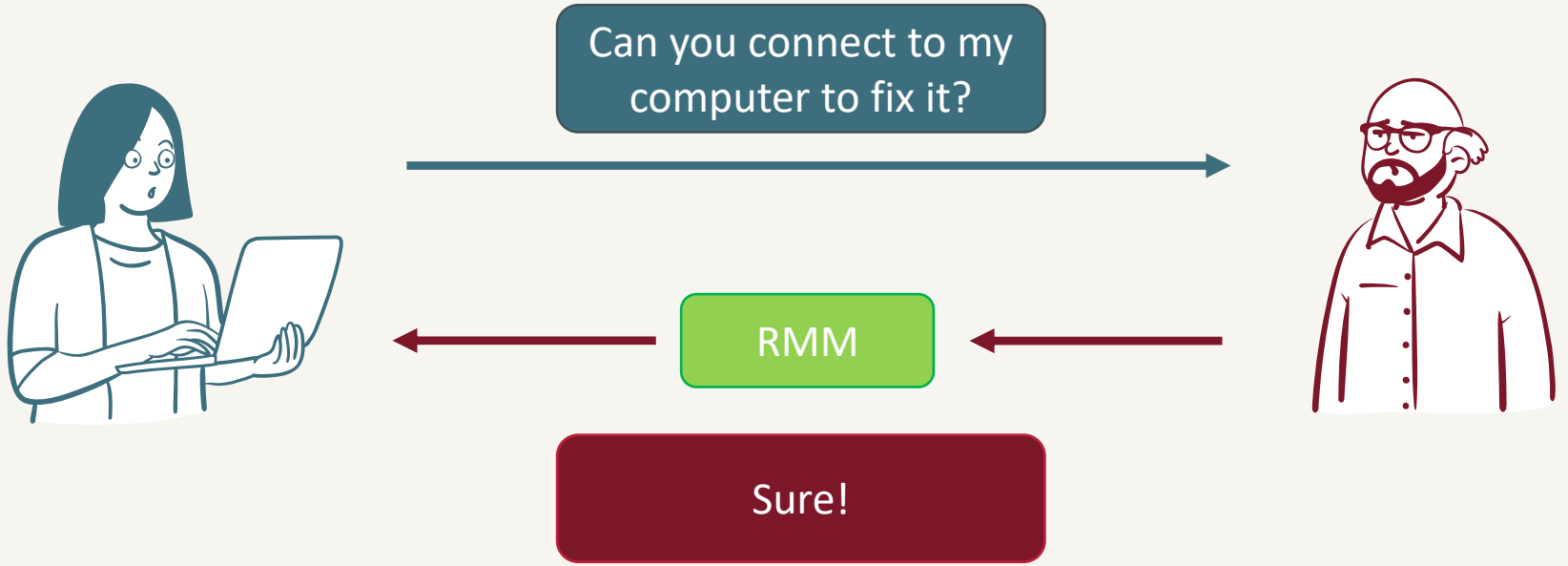
- 25+ years in Information Security and Incident Response
- Extensive experience in leading and responding to a variety of incidents
- Experience in diverse verticals including healthcare, manufacturing, technology, and financial services
- Accomplished speaker and trainer at local, national, and online conferences
- Certs include: GIAC GCFA, GIAC GCFE

Agenda

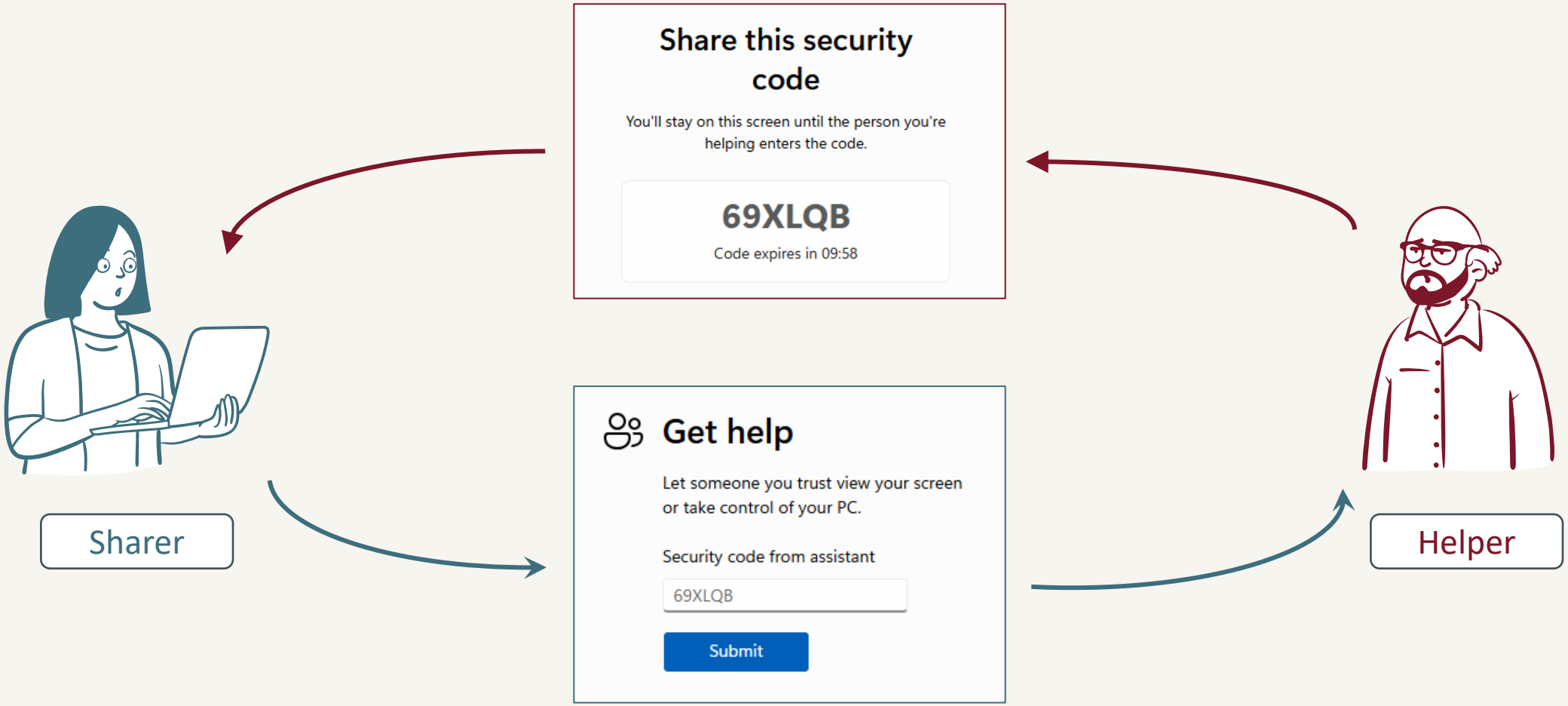
- What is MS Quick Assist?
- Why do we care?
- How does it work?
- Forensic Artifacts
- Forensic Investigations

What are RMMs?

- Remote monitoring and management (RMM) tool
- Enables users to give system access to support to troubleshoot issues

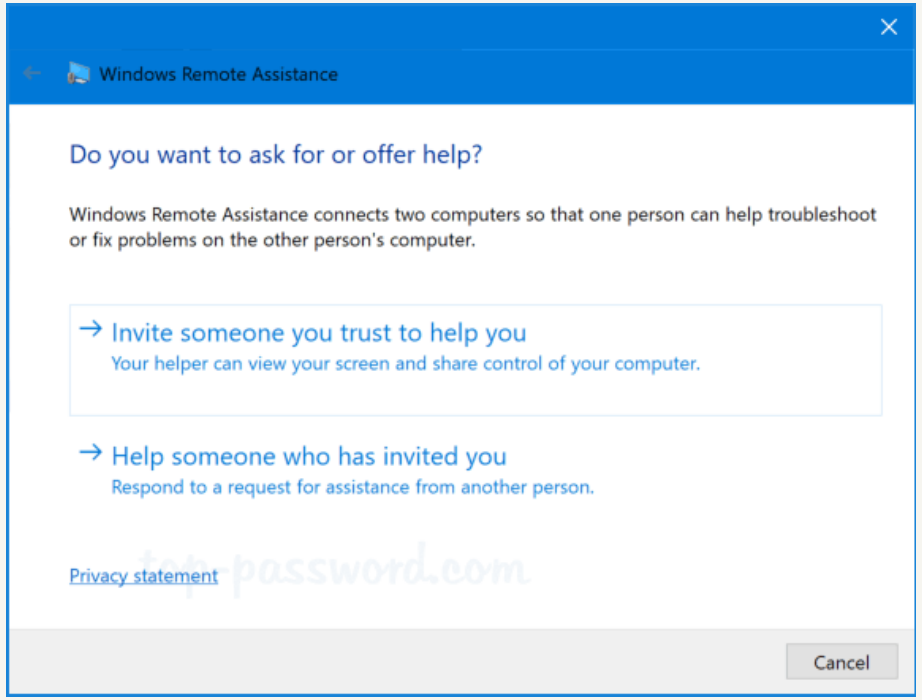


Microsoft Quick Assist



Quick Assist History

- Windows XP – Remote Assistance introduced
  - **Uses RDP – required TCP/3389 to be accessible**
- Windows Vista – Upgraded to have a GUI, additional features
- Quick Assist introduced in Windows 10 Anniversary Update
  - **Remote Assistance still present, but hidden**
- Installed by default on Win 10 Anniversary and Win 11+
- Nov 2021 – Microsoft Intune Remote Help
  - **Business friendly Quick Assist**



Why are we talking about MS Quick Assist?

Microsoft warns of hacker misusing Quick Assist in Black Basta ransomware attacks

Threat researchers say a financially-motivated attacker has deployed the tool in social-engineering attacks since April.

Research Threat intelligence Microsoft Defender Social engineering / phishing

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

By Microsoft Threat Intelligence

Social Engineering RMM Attacks

Quick Assist Operations

From a Forensic Point of View

Quick Assist Limitations

Sharer must consent to letting *helper* control system

Helper can:

Control system (with consent)

Chat

Helper cannot:

Transfer files natively

Copy/paste

Click through UAC prompts

Quick Assist Location

C:\windows\system32\quickassist.exe

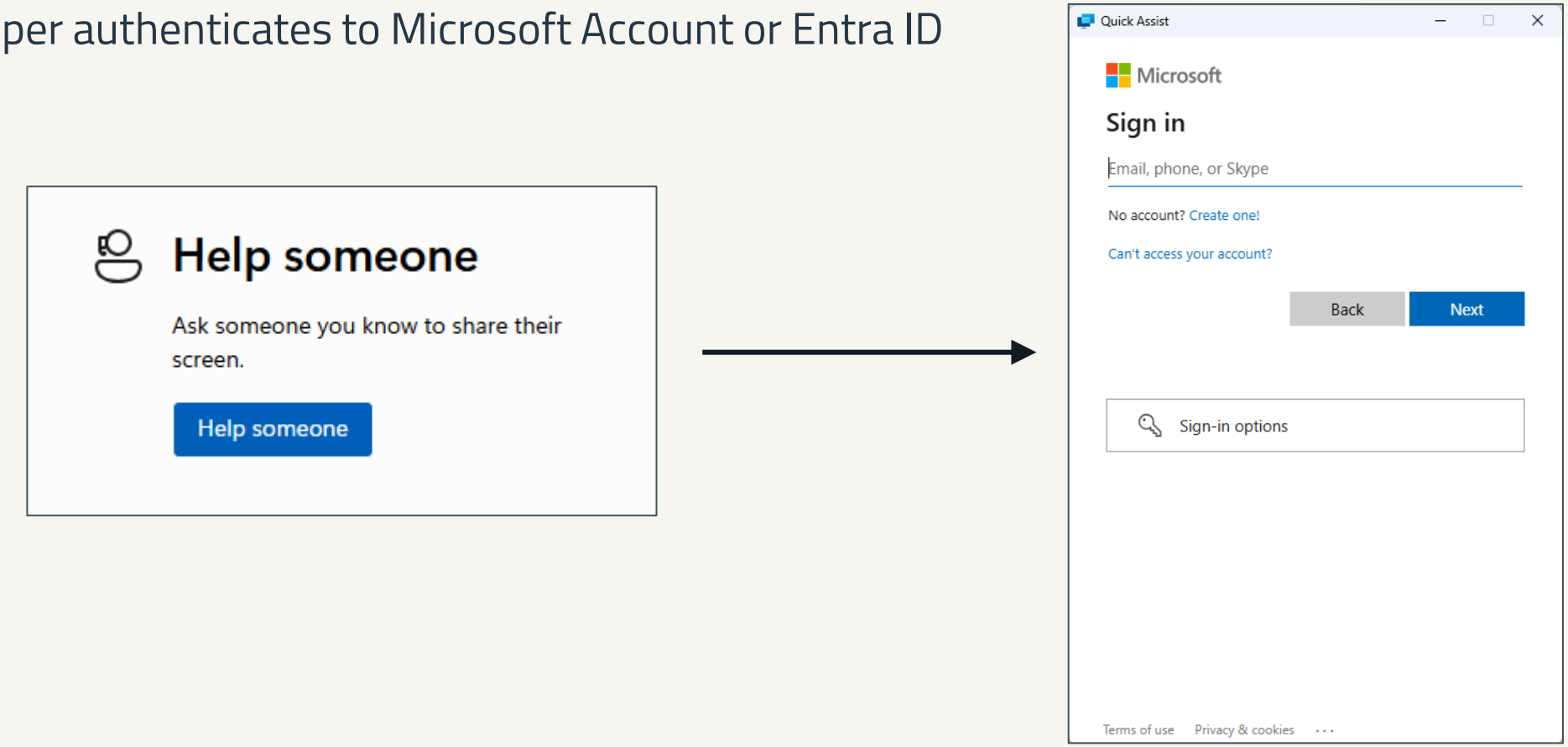
- Location when installed by default
- Mostly Windows 10 systems

C:\Program Files\WindowsApps
MicrosoftCorporationII.QuickAssist_[VERSION]__ 8wekyb3d8bbwe
Microsoft.RemoteAssistance.QuickAssist\QuickAssist.exe

- [VERSION] is QA version #
- Windows 11 default installs and installed from Microsoft Store

Authentication

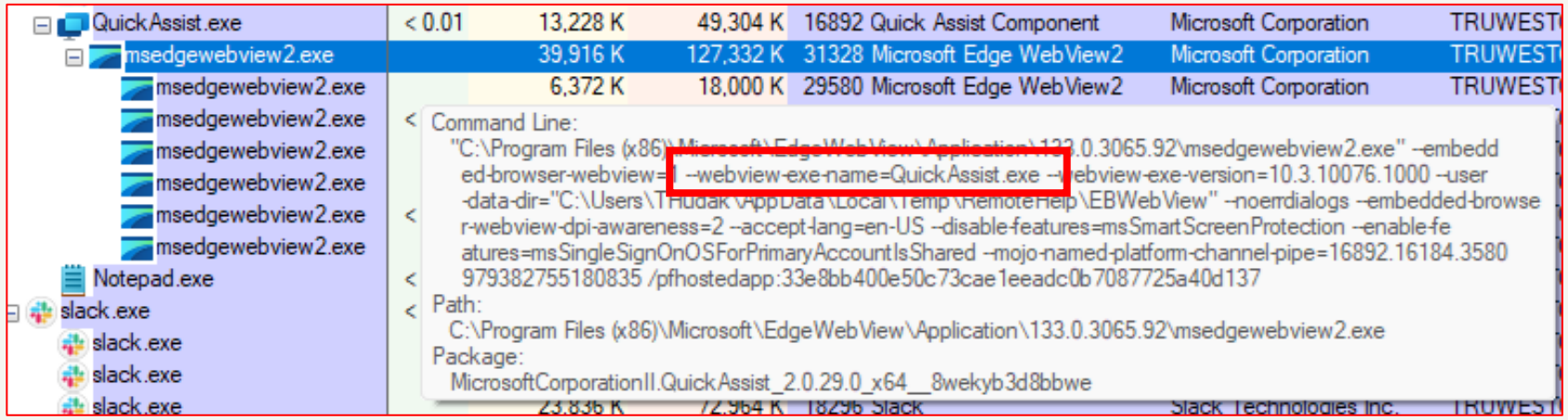
- Sharer is logged into their computer already
- Helper authenticates to Microsoft Account or Entra ID



Initial Execution Flow

User runs Quick Assist

quickassist.exe



msedgewebview2.exe **--webview-exe-name=quickassist.exe**

Many msedgewebview2.exe

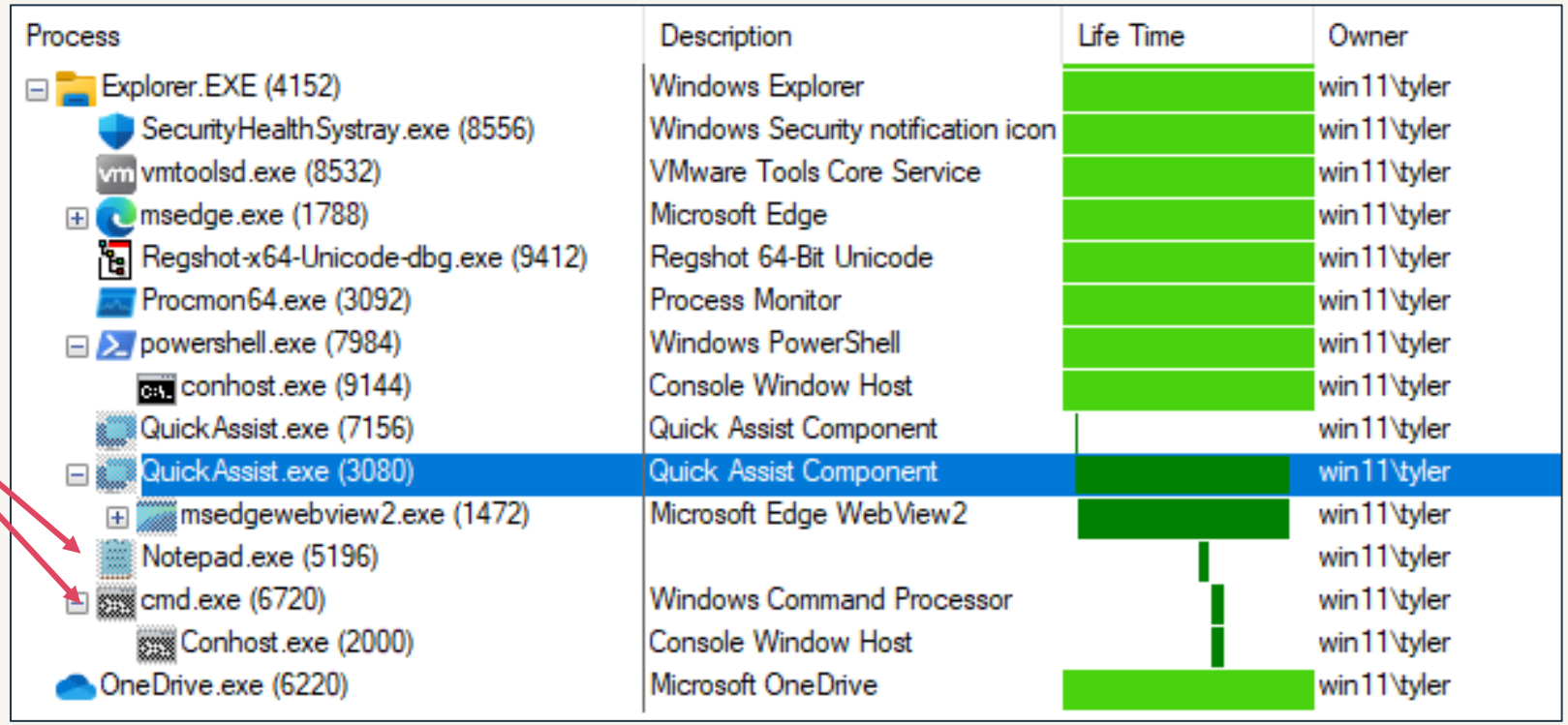
May have “webview-exe-name” (or not)

Execution of Programs

- Programs executed in QA session are done under normal Windows parent-child
- NOT under quickassist.exe or msedgewebview2.exe

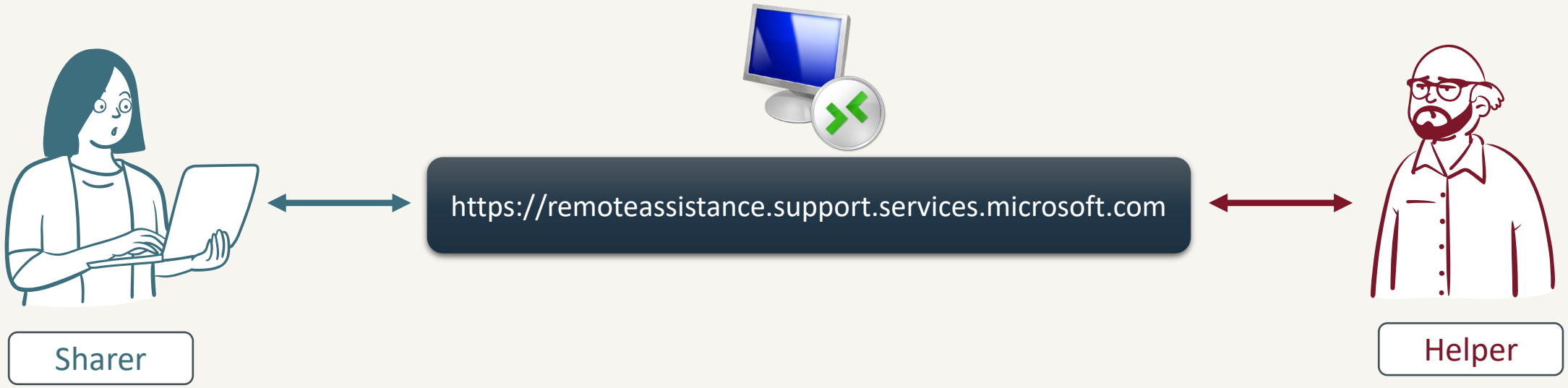
Executed in QA session

Parent is Explorer.exe



Network Communications

- Remote Desktop Protocol (RDP) is the underlying protocol
- Communicates over TCP/443 (TLS 1.2) not TCP/3389



URL	Description
.microsoft.com	Accessible Rich Internet Applications (ARIA) service for providing accessible experiences to users.
*.cc.skype.com	Required for Azure Communication Service.
*.events.data.microsoft.com	Required diagnostic data for client and services used by Quick Assist.
*.flightproxy.skype.com	Required for Azure Communication Service.
*.live.com	Required for logging in to the application (MSA).
*.monitor.azure.com	Required for telemetry and remote service initialization.
*.registrar.skype.com	Required for Azure Communication Service.
*.support.services.microsoft.com	Primary endpoint used for Quick Assist application
*.trouter.skype.com	Used for Azure Communication Service for chat and connection between parties.
aadcdn.msauth.net	Required for logging in to the application (Microsoft Entra ID).
edge.skype.com	Used for Azure Communication Service for chat and connection between parties.
login.microsoftonline.com	Required for Microsoft sign-in service.
remoteassistanceprodacs.communication.azure.com	Used for Azure Communication Service for chat and connection between parties.
turn.azure.com	Required for Azure Communication Service.

Quick Assist Forensic Analysis

Forensic Investigation Questions…

Is this the Helper or Sharer's PC?

When did QA session start? End?

Was consent given?

User / IP Address of Helper

What did Helper execute/access/etc.?

Event Logs

System32 Version

- Nothing

Win11 / Microsoft Store Version

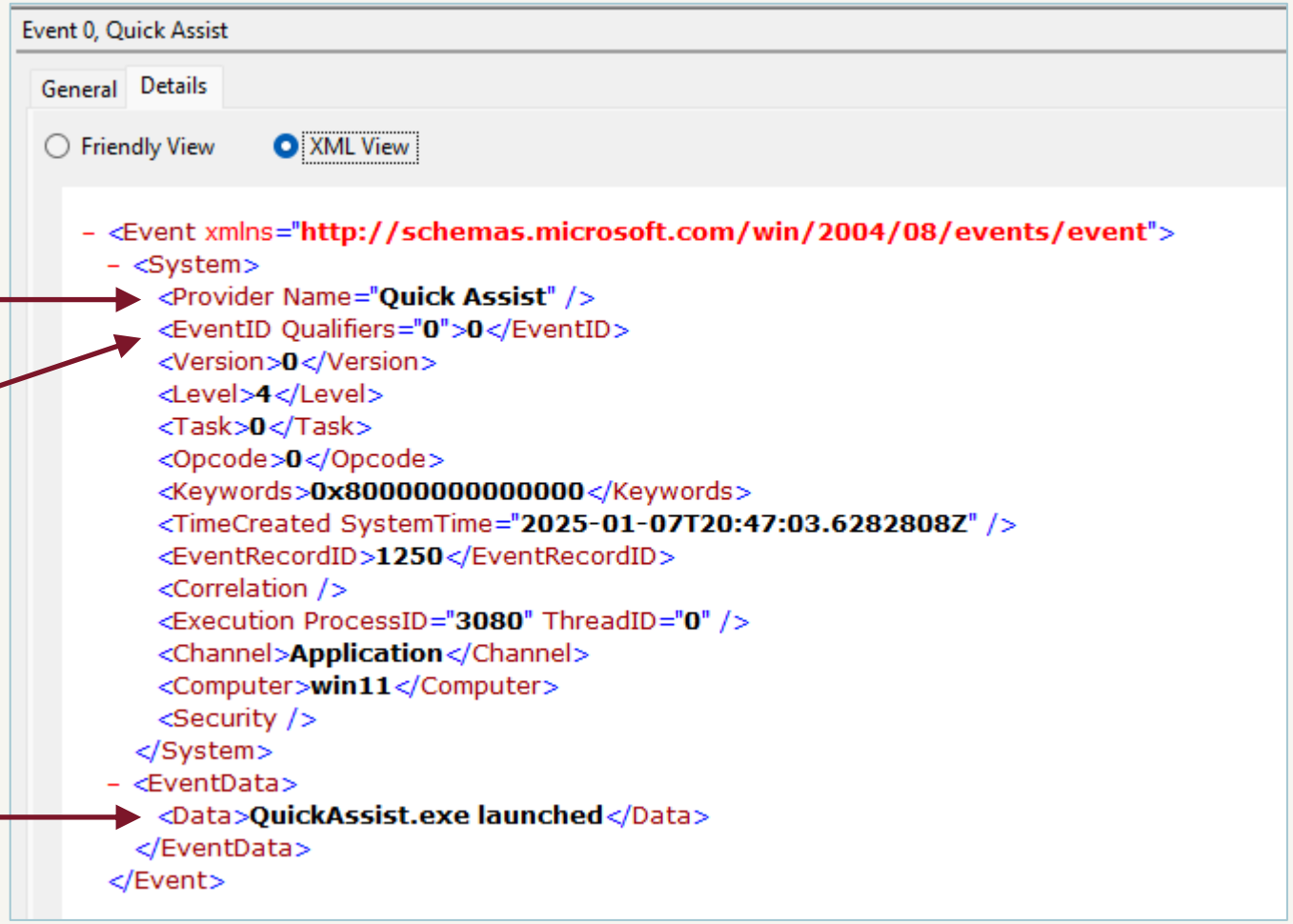
- Logged into Application.evtx
- Under “Quick Assist” Source
- All are event ID 0
- No defined structure – feel like debug and error messages (or a mistake)

Application Event Logs

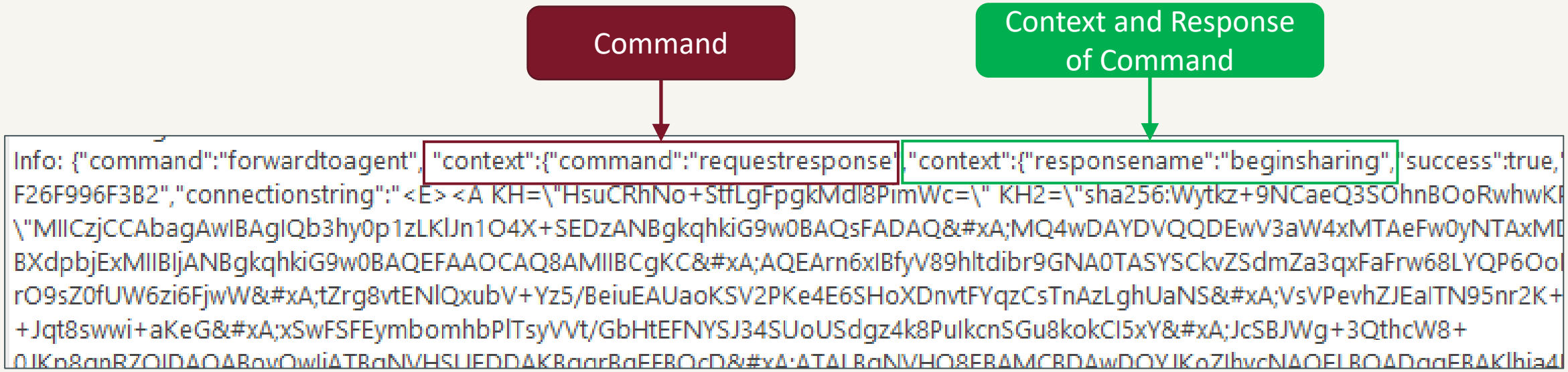
Event Source

Event ID

QA Start of Execution

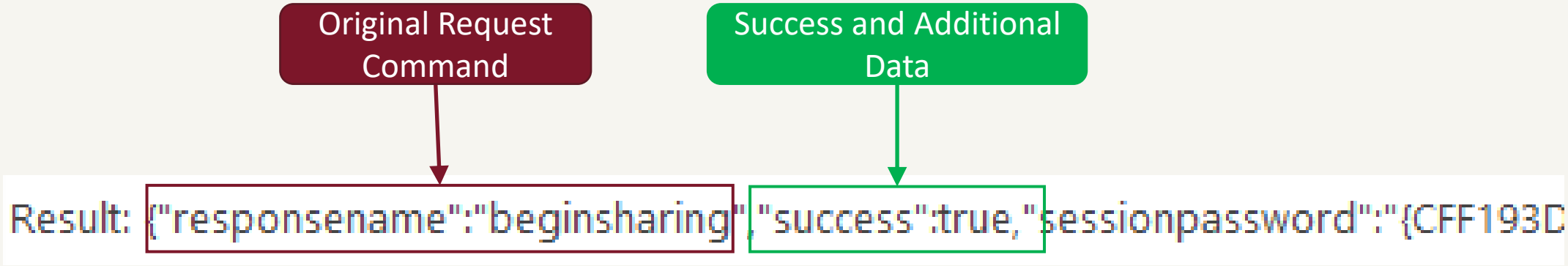


JSON Event Logs - Request



- Context Command “requestresponse” is request for action
- “context:responsename” contains info on the request/response or success
- Not everything is logged or may be truncated

JSON Event Logs - Response



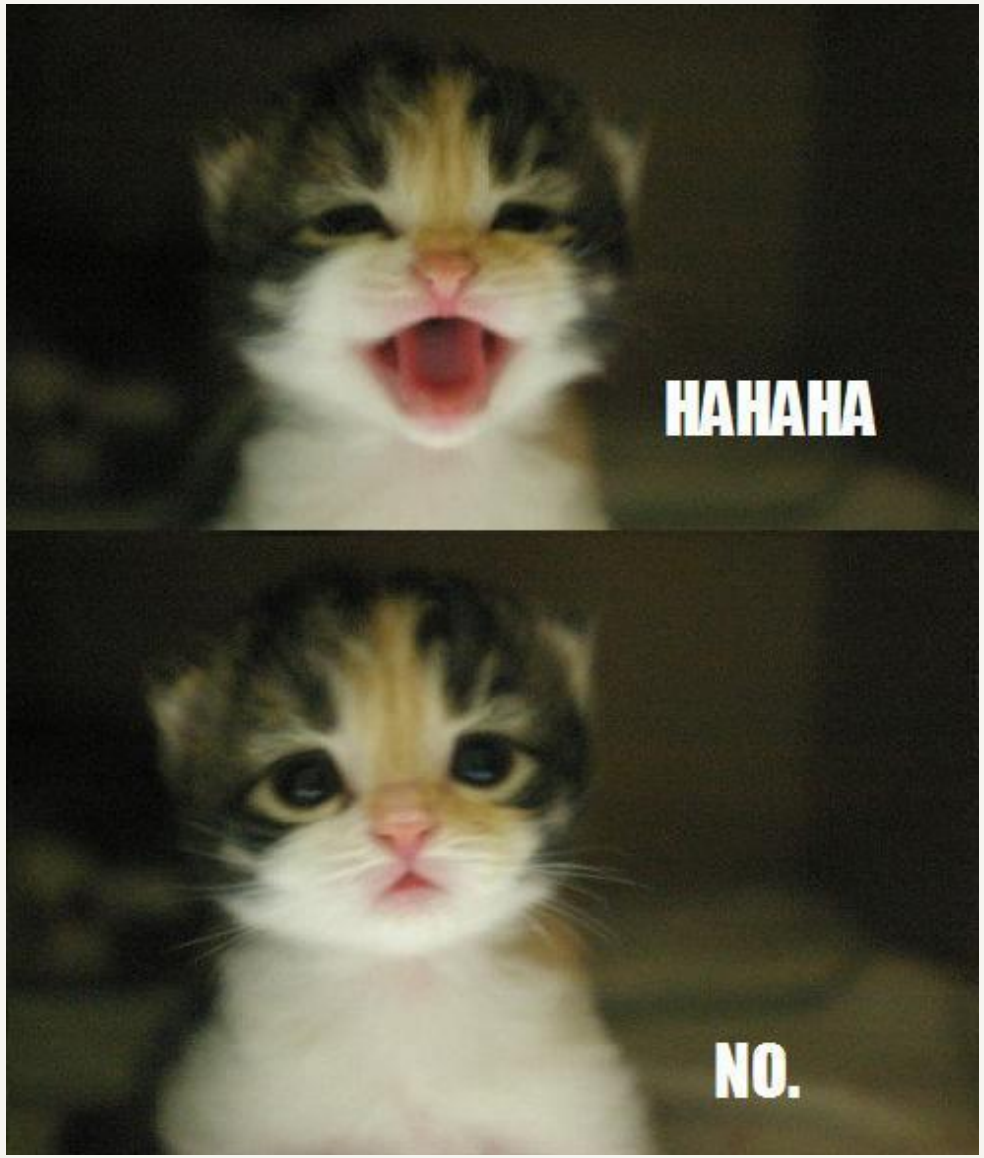
- “responsename” contains original request command
- Additional data and success follows

Quick Assist Event Log Messages

Event	Request Context ResponseName	Context Info
Quick Assist Launched	*QuickAssist.exe Launched*	
Sharer shared screen with Helper	beginsharing	
Sharer gives Consent to Helper	setsharingmode	SharingMode: FullControl
Control is cancelled or removed	setsharingmode	SharingMode: View
Sharing stops	endsharing	
Quick Assist closed	sendappclose	

Surely the QA connection creates an auth event?

A Security.evtx 4624, right?



File System Artifacts - Sharer

- \ProgramData\Packages\MicrosoftCorporationII.QuickAssist_8wekyb3d8bbwe*[SID]*\SystemAppData\Helium
  - **SID is user who ran Quick Assist**
- %USER%\AppData\Local\Packages\MicrosoftCorporationII.QuickAssist_8wekyb3d8bbwe\SystemAppData\Helium\
  - **Registry files, nothing useful inside (so far)**
- C:\Users\All Users\Packages\MicrosoftCorporationII.QuickAssist_8wekyb3d8bbwe*[SID]*\SystemAppData\Helium\
  - **Registry files, nothing useful inside (so far)**

%APPDATA%\Local\Temp\RemoteHelp\EBWebView (Sharer)

- MS Edge Cache Files from msedgewebview2.exe
- Analyze with Hindsight (https://github.com/obsidianforensics/hindsight)
- *https://remoteassistance.support.services.microsoft.com*
  - **First instance occurs shortly after QA launched**
- *https://remoteassistance.support.services.microsoft.com/screenshare*
  - **Shortly after screen sharing enabled or sharing code is entered**
- *https://remoteassistance.support.services.microsoft.com/status/ended*
  - **Sharing connection has been closed**

Type	Timestamp (UTC)	URL	Title / Name / Status
preference (session)	2025-01-07 20:47:05.095		Session event log [in Prefere
site setting (dips)	2025-01-07 20:47:07.348	microsoft.com	first_site_storage_time
url	2025-01-07 20:47:07.399	https://remoteassistance.support.services.microsoft.com/	Microsoft Quick Assist
site setting (modified)	2025-01-07 20:47:07.400	https://[*.]microsoft.com,*	cookie_controls_metadata [i
url	2025-01-07 20:47:24.148	https://remoteassistance.support.services.microsoft.com/screenshare	Microsoft Quick Assist

RDP Artifacts

- No Microsoft-Windows-TerminalServices* event logs are created on either side
- RDP Cache is created on Helper
  - **%USER%\AppData\Local\Packages\MicrosoftCorporationII.QuickAssist_8wekyb3d8bbwe\LocalCache\Local\Microsoft\Terminal Server Client\Cache\bcache24.bmc**
- Reconstruction Tools:
  - **BMC-Tools - https://github.com/ANSSI-FR/bmc-tools**
  - **RDP Cache Stitcher - https://github.com/BSI-Bund/RdpCacheStitcher**
  - **RDPieces - https://github.com/brimorlabs/rdpieces**

Registry Artifacts - Sharer

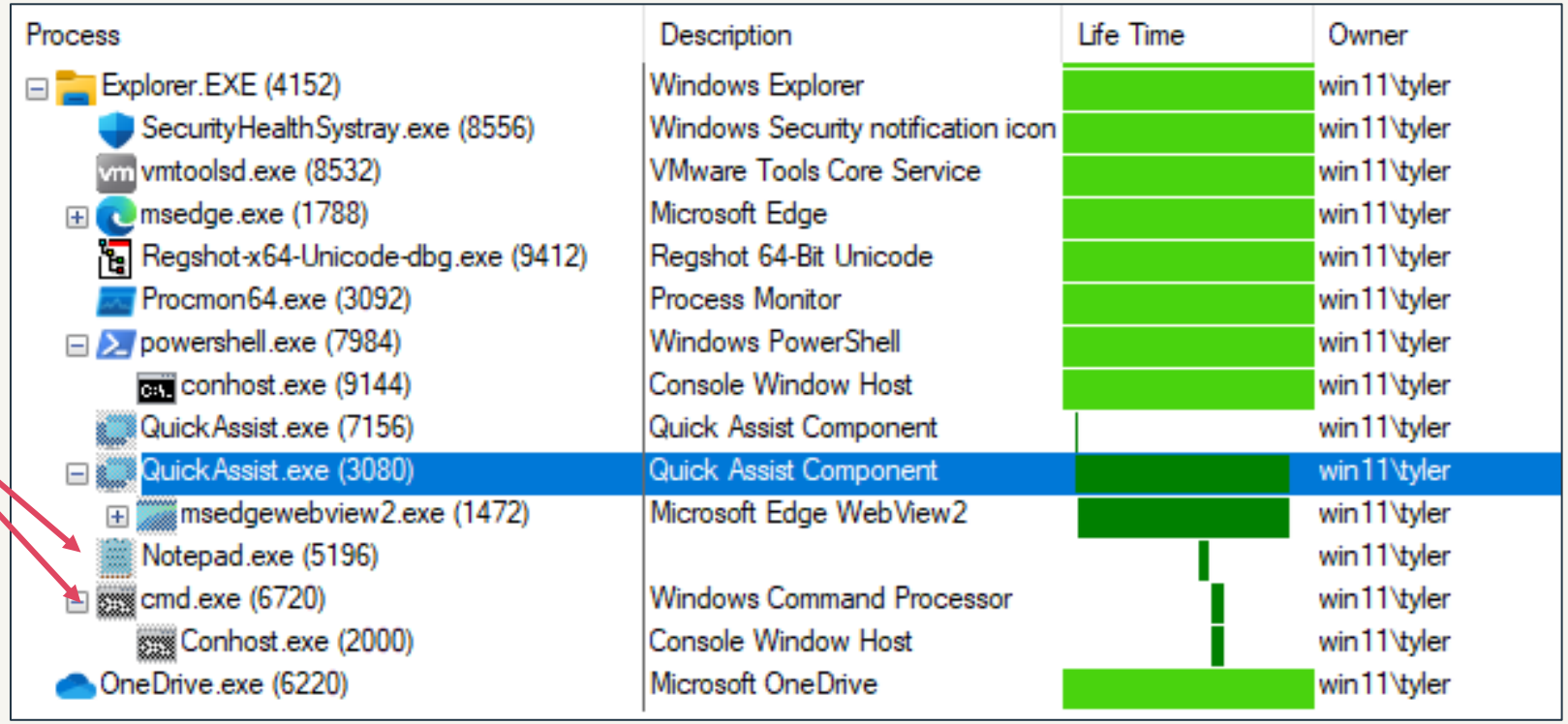
Key	Value	Data	Notes
HKCU\Software\Classes\Local Settings\Software\Microsoft\ Windows\CurrentVersion\ AppModel\SystemAppData\ MicrosoftCorporationII.QuickAssist_8wekyb3 d8bbwe	WasEverActivated	1	Indicates use of QuickAssist
…\HAM\AUI\App\V1\LU\	PCT PTT	(hex)	Unknown purpose

Look at Registry key last modified time for last QA execution

Execution Artifacts

Executed in QA session

Parent is Explorer.exe



Process	Description	Life Time	Owner
Explorer.EXE (4152)	Windows Explorer		win11\tyler
SecurityHealthSystray.exe (8556)	Windows Security notification icon		win11\tyler
vmtoolsd.exe (8532)	VMware Tools Core Service		win11\tyler
msedge.exe (1788)	Microsoft Edge		win11\tyler
Regshot-x64-Unicode-dbg.exe (9412)	Regshot 64-Bit Unicode		win11\tyler
Procmon64.exe (3092)	Process Monitor		win11\tyler
powershell.exe (7984)	Windows PowerShell		win11\tyler
conhost.exe (9144)	Console Window Host		win11\tyler
QuickAssist.exe (7156)	Quick Assist Component		win11\tyler
QuickAssist.exe (3080)	Quick Assist Component		win11\tyler
msedgewebview2.exe (1472)	Microsoft Edge WebView2		win11\tyler
Notepad.exe (5196)			win11\tyler
cmd.exe (6720)	Windows Command Processor		win11\tyler
Conhost.exe (2000)	Console Window Host		win11\tyler
OneDrive.exe (6220)	Microsoft OneDrive		win11\tyler

Execution Artifacts

Executed programs in QA session are in normal Windows parent/child relationship

↓

All executed processes will be under the Sharer's ID

↓

Process execution logging will NOT show what was executed by the helper

Determining Attacker Actions

1. Find start of QA session

- Event logs – Sec 4688, Sysmon 1 for QuickAssist.exe
- Application event log Quick Assist source “Quick Assist Launched”
- QA MS Edge history files
- Prefetch for QuickAssist.exe
- Creation times of file system artifacts
- Network activity to known domains

2. Find stop of QA session

- Application event log Quick Assist source
  - endsharing or sendappclose context
- QA MS Edge history files
- Last mod time of file system artifacts

Determining Attacker Actions

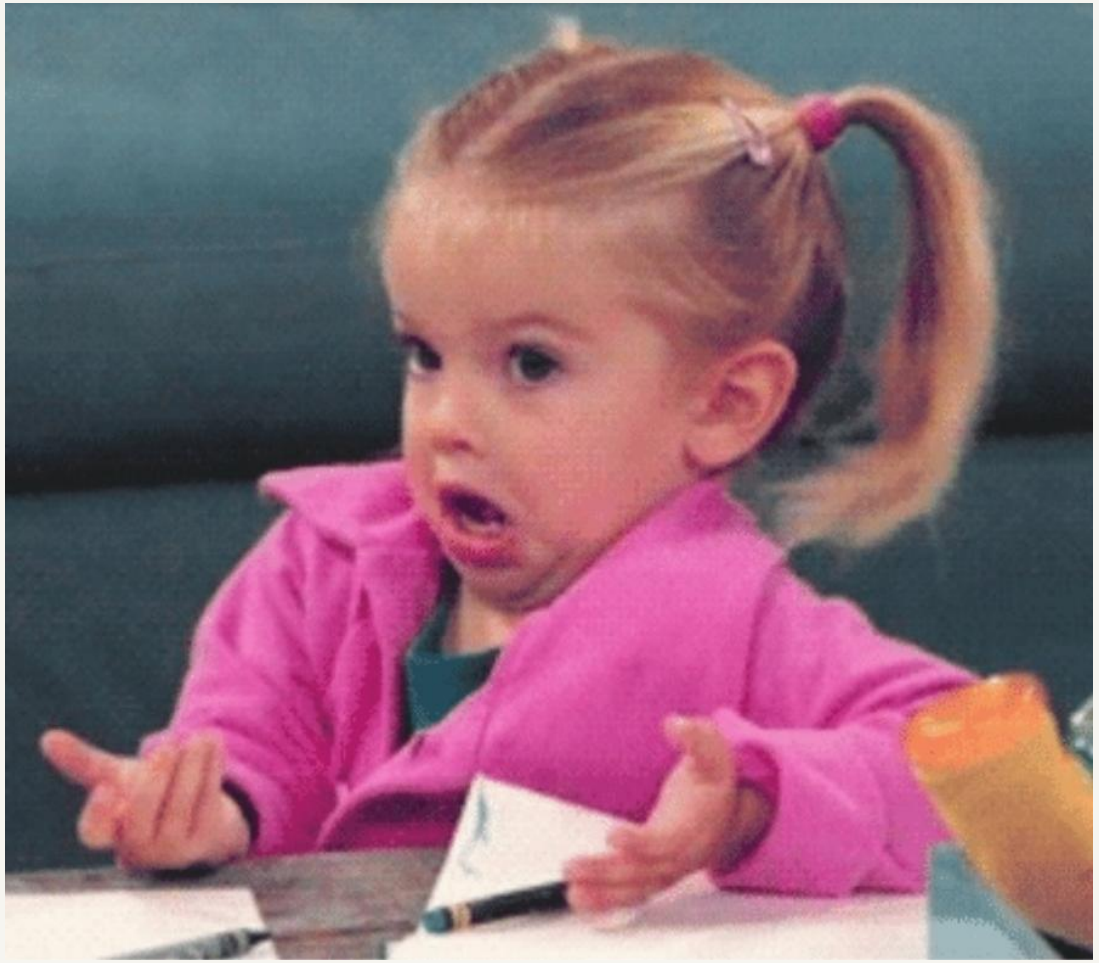
3. Obtain “normal” evidence of execution artifacts

- Prefetch, SRUM
- Sec 4688 / Sysmon 1
- Registry: AmCache, UserAssist, BAM, MUICache, etc.

4. What falls in between the start and stop times?

- Take into context what was executed
- Talk to the victim

Network Artifacts



- Traffic:
  - Goes through Microsoft's servers
  - Encrypted
- Network telemetry reflects this
- Microsoft might have data, but only for a limited time

> **Note**
>
> No logs are created on either the helper's or sharer's device. Microsoft can't access a session or view any actions or keystrokes that occur in the session.
>
> The sharer sees only an abbreviated version of the helper's name (first name, last initial) and no other information about them. Microsoft doesn't store any data about either the sharer or the helper for longer than three days.

Forensic Investigation Questions…

Is this the Helper or Sharer's PC? ✓

When did QA session start? End? ✓

Was consent given? ✓

User / IP Address of Helper ✗

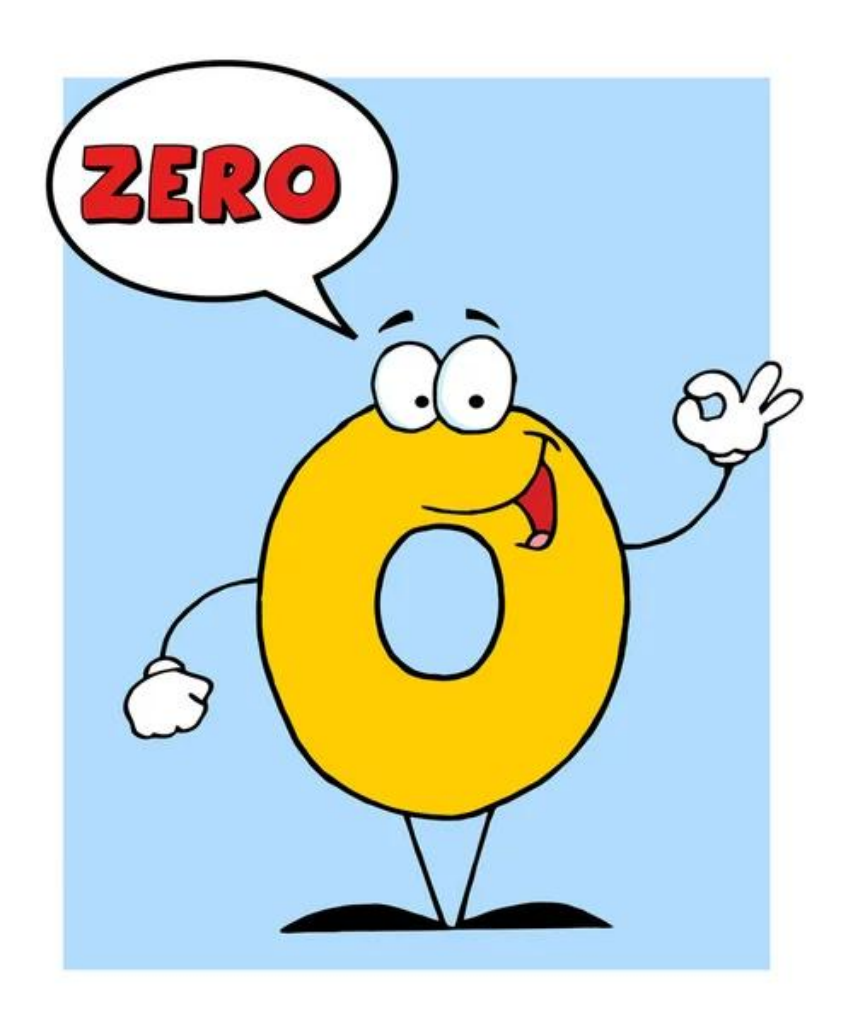
What did Helper execute/access? ?

Prevention

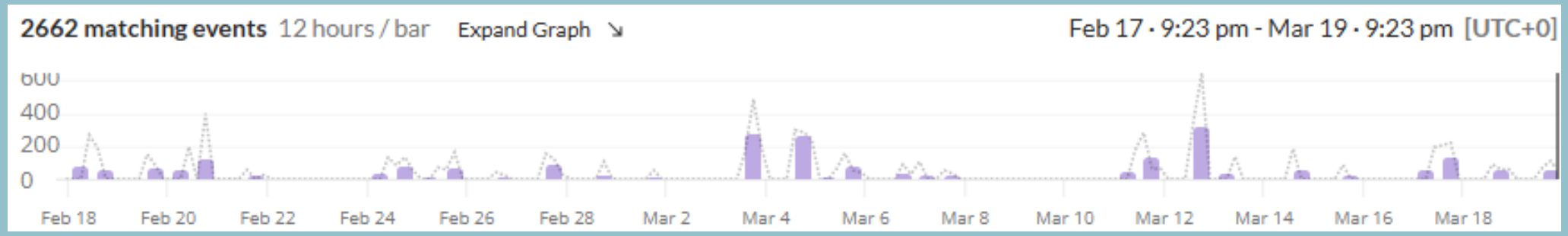
Quick Assist Access Controls

No native access controls

Unless you buy MS Intune Remote Help



- Block access to https://remoteassistance.support.services.microsoft.com
  - Also blocks MS Intune Remote Help
- Uninstall and/or delete Quick Assist
  - Need it? Upgrade to MS Store version
- Denylist Quick Assist
- Monitor for Quick Assist execution



Resources

- Investigating Microsoft Quick Assist:
  - **https://hackuponthegale.github.io/blog/dfir/QuickAssist1**
- LOLRMM
  - **https://lolrmm.io/tools/quick_assist**
- Strontic xCyclopedia
  - **https://strontic.github.io/xcyclopedia/library/quickassist.exe-39AB5ED601B0C39DCE3B7D269847C944.html**
- Microsoft Quick Assist
  - **https://learn.microsoft.com/en-us/windows/client-management/client-tools/quick-assist**

Thank you!

Tyler Hudak
Tyler.Hudak@inversion6.com
@secshoggoth