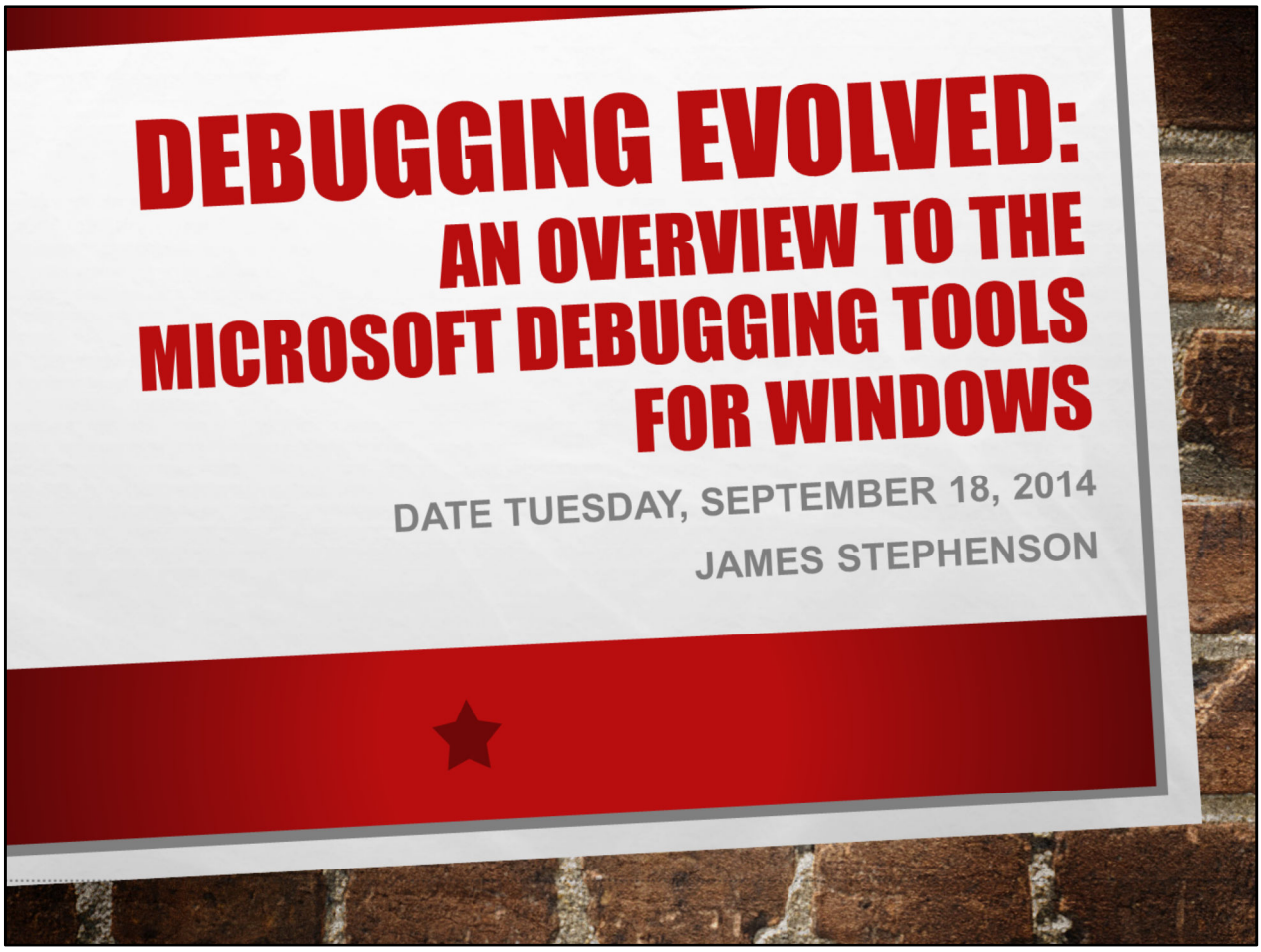
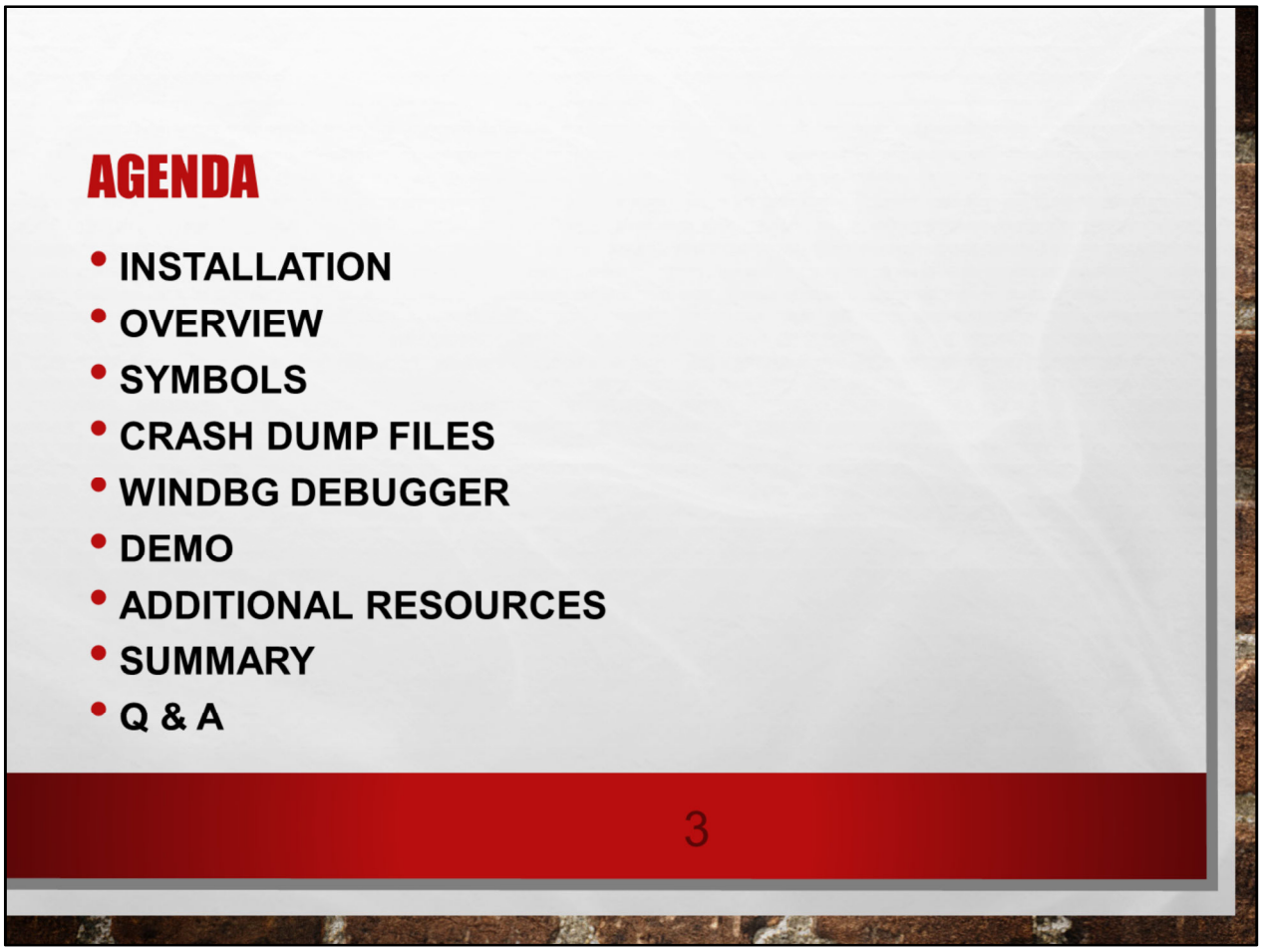

DEBUGGING EVOLVED:
AN OVERVIEW TO THE MICROSOFT DEBUGGING TOOLS FOR WINDOWS
DATE TUESDAY, SEPTEMBER 18, 2014
JAMES STEPHENSON

JAMES STEPHENSON

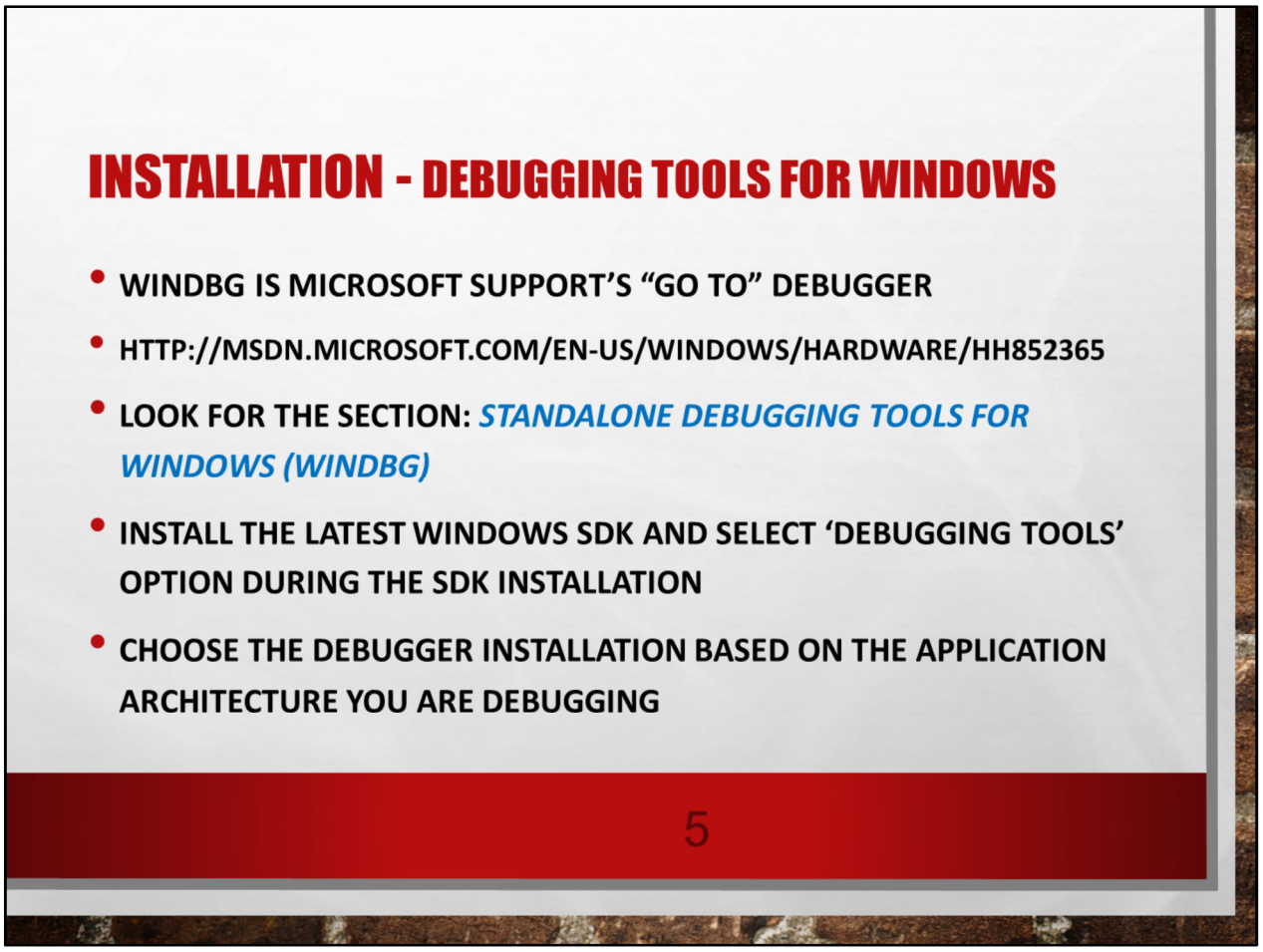
James is an application development manager with extensive experience in software engineering management, software architectures and delivering Windows and web point of sale software solutions for agents to illustrate life, annuity and group products for the Insurance industry. He's known for leading the transformation of a small on-shore product development team to an agile, globally distributed, high-performance team delivering virtualized Cloud-based products and services organization. James is a Miami native who enjoys travel, boating, technology and cooking.

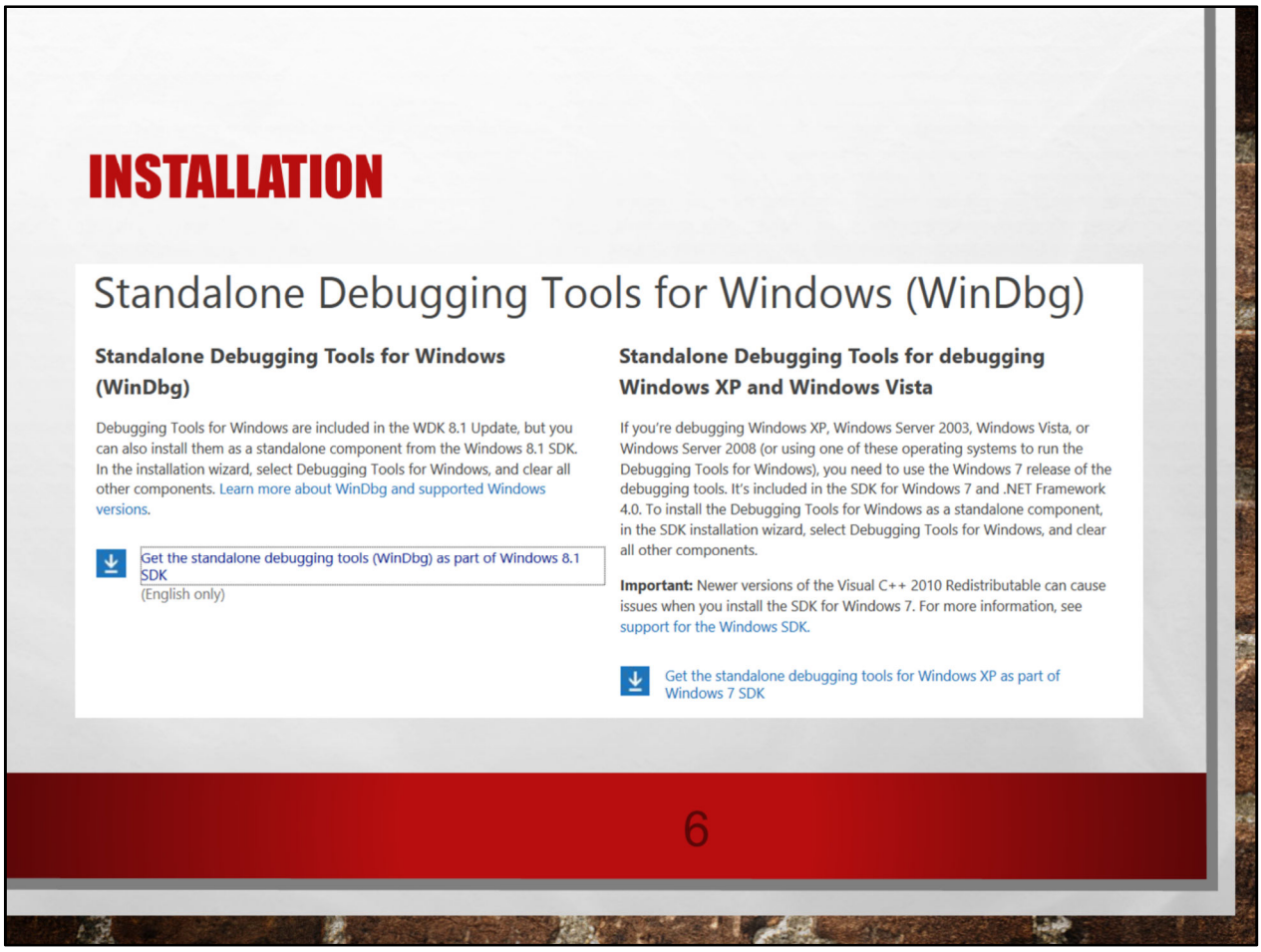
jamesgstephenson@gmail.com
https://www.linkedin.com/in/jamesgstephenson

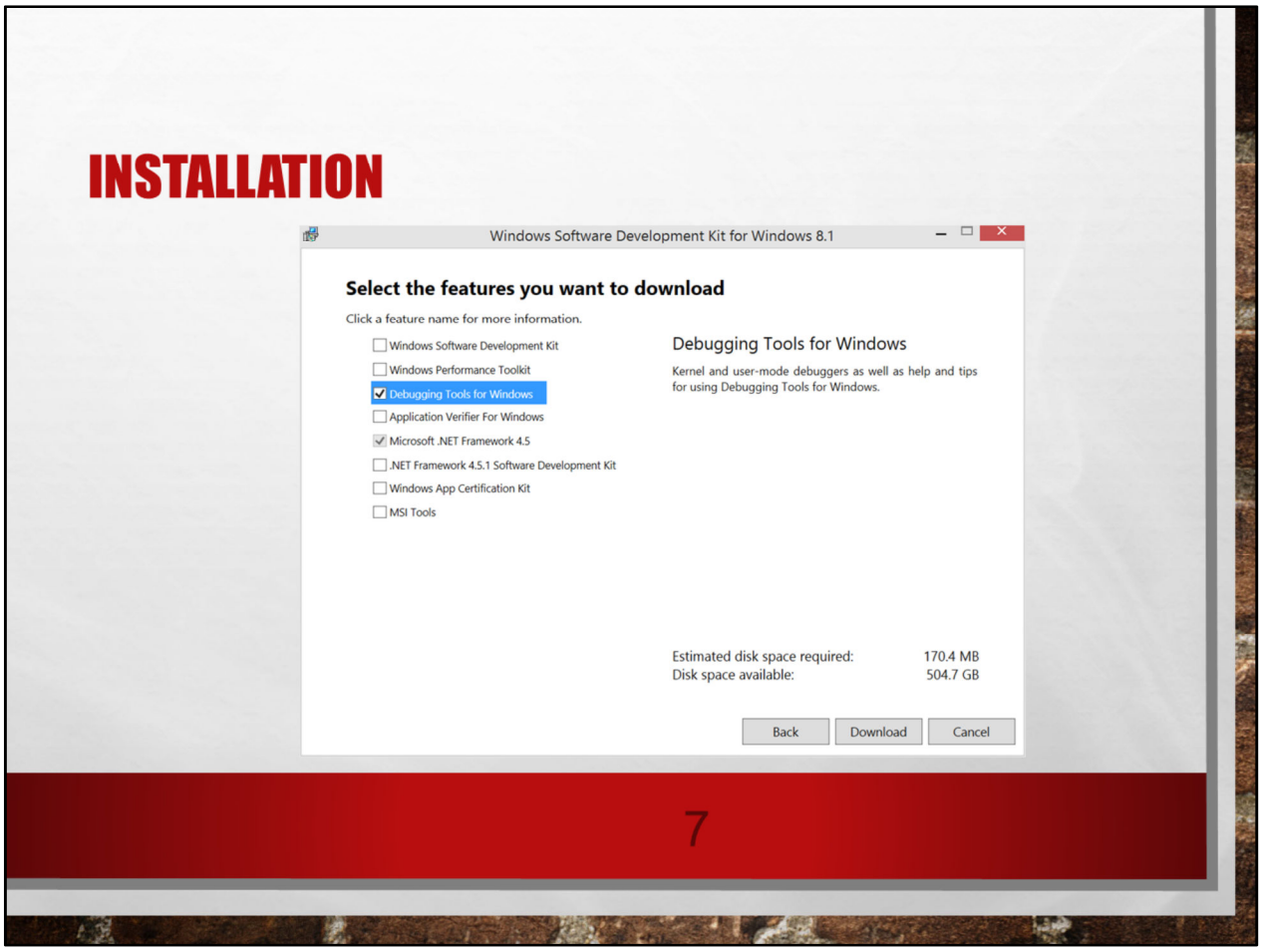
2


AGENDA
INSTALLATION
OVERVIEW
SYMBOLS
CRASH DUMP FILES
WINDBG DEBUGGER
DEMO
ADDITIONAL RESOURCES
SUMMARY
Q & A
3

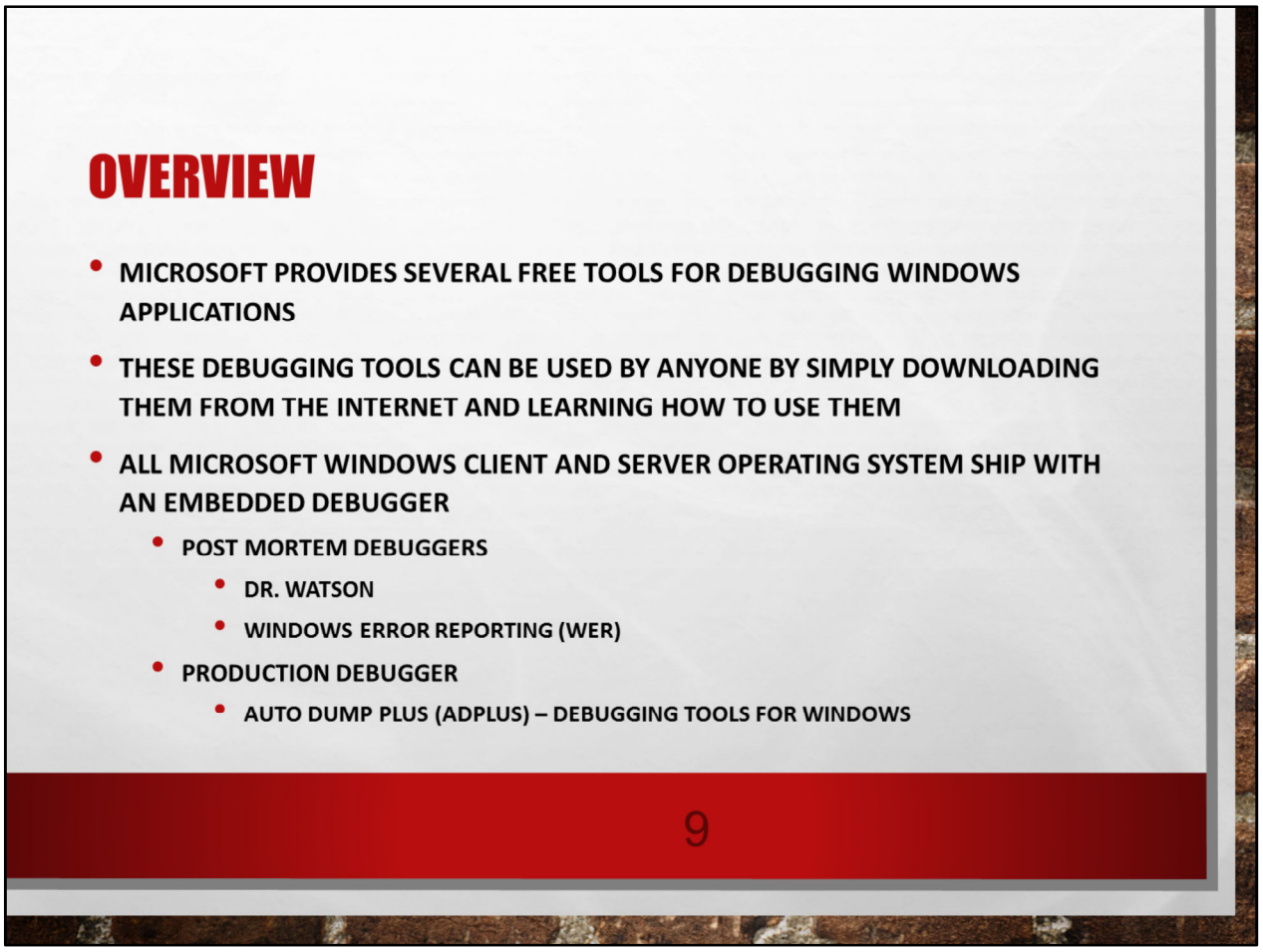

Installation


INSTALLATION - DEBUGGING TOOLS FOR WINDOWS
WINDBG IS MICROSOFT SUPPORT'S "GO TO" DEBUGGER
HTTP://MSDN.MICROSOFT.COM/EN-US/WINDOWS/HARDWARE/HH852365
LOOK FOR THE SECTION: STANDALONE DEBUGGING TOOLS FOR WINDOWS (WINDBG)
INSTALL THE LATEST WINDOWS SDK AND SELECT 'DEBUGGING TOOLS' OPTION DURING THE SDK INSTALLATION
CHOOSE THE DEBUGGER INSTALLATION BASED ON THE APPLICATION ARCHITECTURE YOU ARE DEBUGGING
5

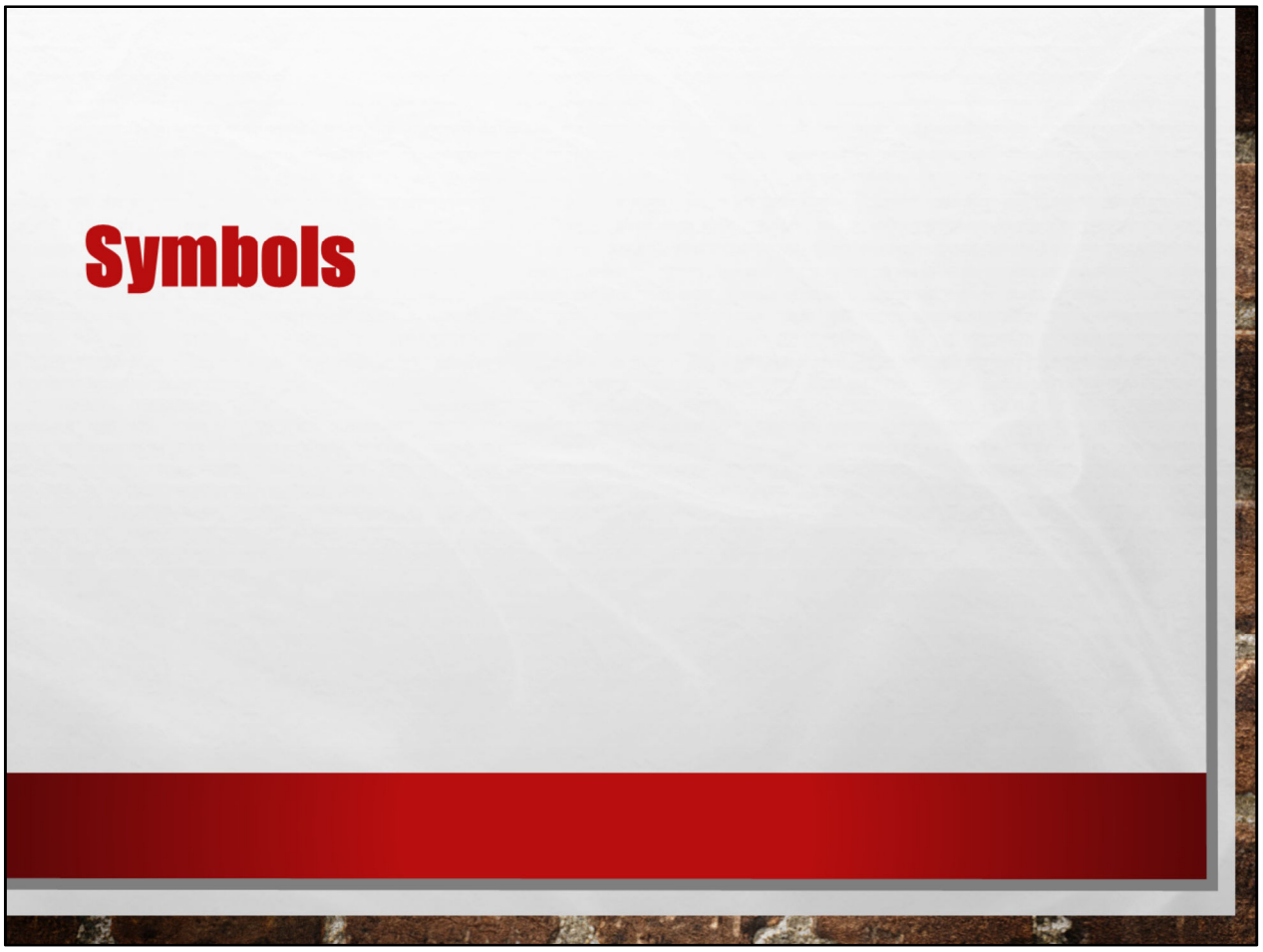

INSTALLATION
Standalone Debugging Tools for Windows (WinDbg)
Standalone Debugging Tools for Windows (WinDbg)
Debugging Tools for Windows are included in the WDK 8.1 Update, but you can also install them as a standalone component from the Windows 8.1 SDK. In the installation wizard, select Debugging Tools for Windows, and clear all other components. Learn more about WinDbg and supported Windows versions.
Get the standalone debugging tools (WinDbg) as part of Windows 8.1 SDK
(English only)
Standalone Debugging Tools for debugging Windows XP and Windows Vista
If you're debugging Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008 (or using one of these operating systems to run the Debugging Tools for Windows), you need to use the Windows 7 release of the debugging tools. It's included in the SDK for Windows 7 and .NET Framework 4.0. To install the Debugging Tools for Windows as a standalone component, in the SDK installation wizard, select Debugging Tools for Windows, and clear all other components.
Important: Newer versions of the Visual C++ 2010 Redistributable can cause issues when you install the SDK for Windows 7. For more information, see support for the Windows SDK.
Get the standalone debugging tools for Windows XP as part of Windows 7 SDK
6

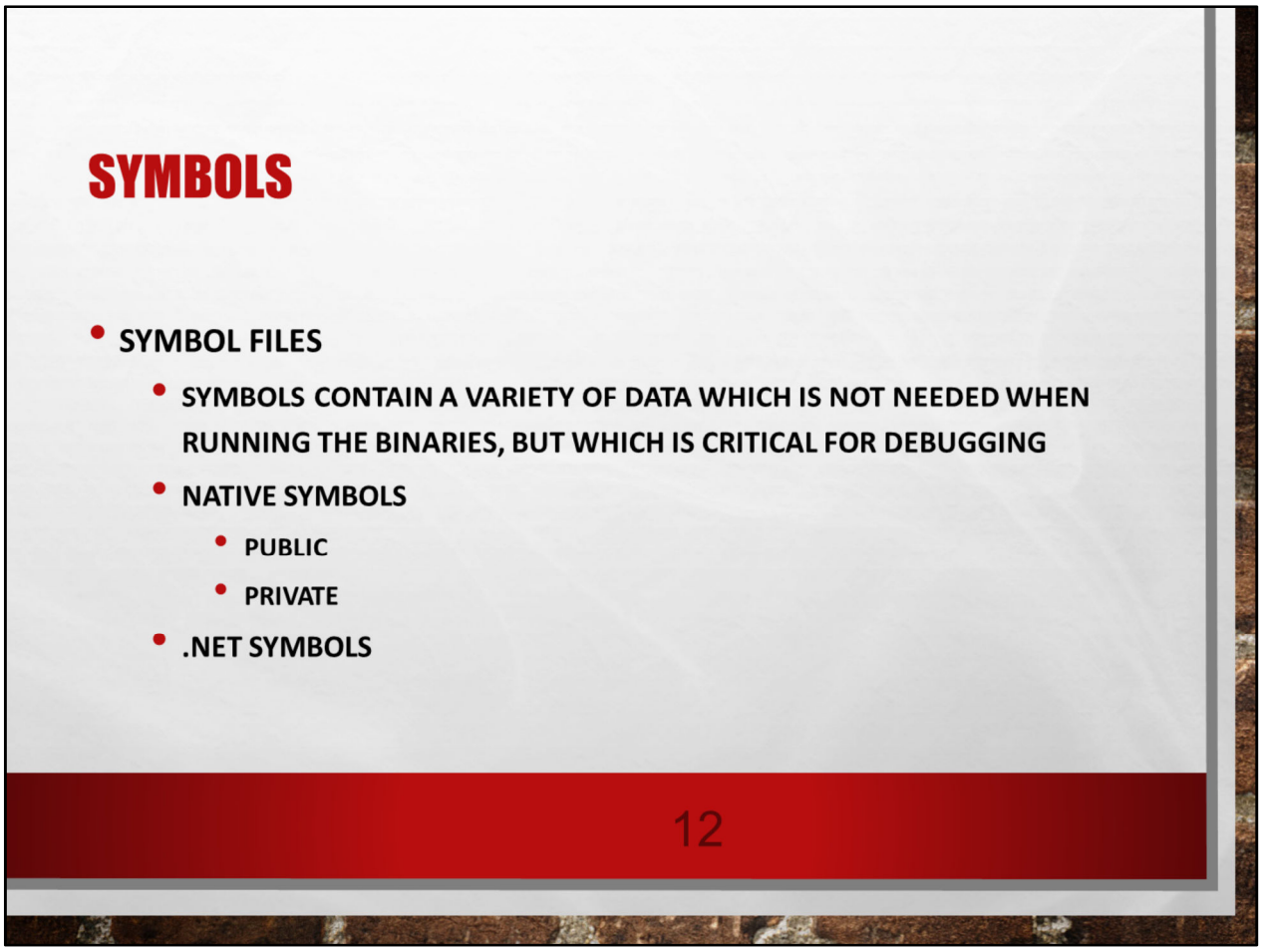

INSTALLATION
Windows Software Development Kit for Windows 8.1
Select the features you want to download
Click a feature name for more information.
Windows Software Development Kit
Windows Performance Toolkit
Debugging Tools for Windows
Application Verifier For Windows
Microsoft .NET Framework 4.5
.NET Framework 4.5.1 Software Development Kit
Windows App Certification Kit
MSI Tools
Debugging Tools for Windows
Kernel and user-mode debuggers as well as help and tips for using Debugging Tools for Windows.
Estimated disk space required: 170.4 MB
Disk space available: 504.7 GB
Back
Download
Cancel
7

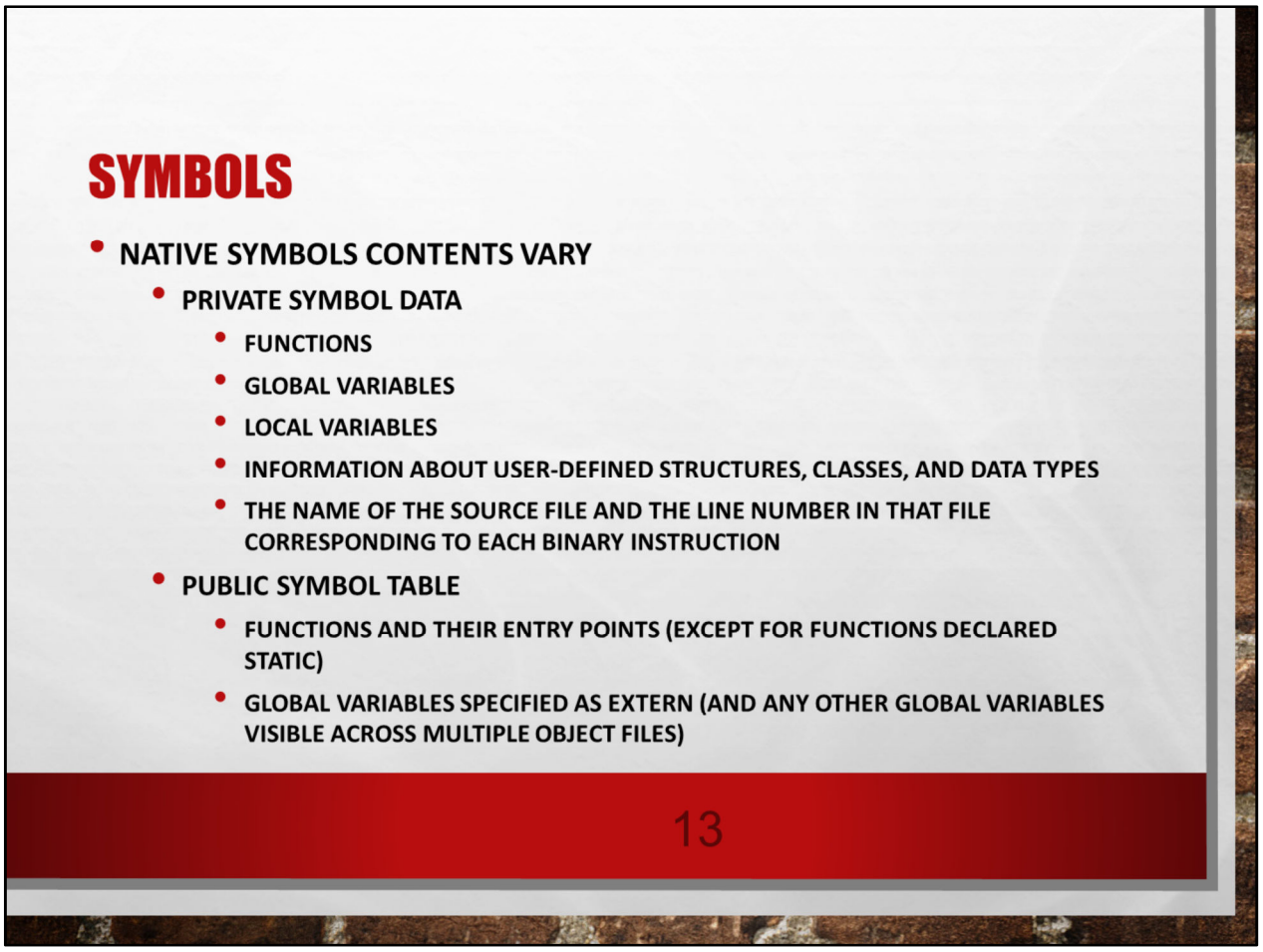

Overview

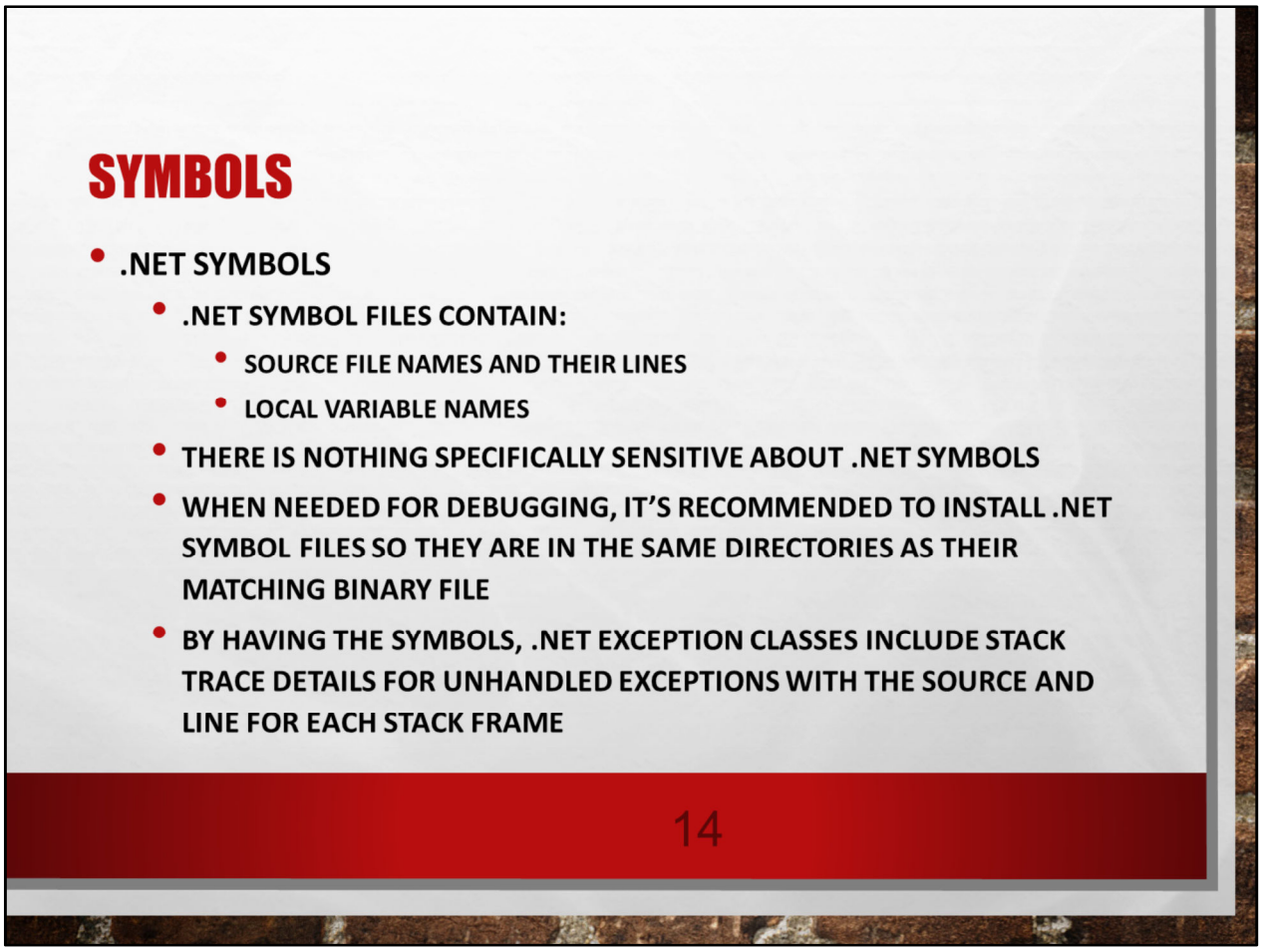

OVERVIEW
MICROSOFT PROVIDES SEVERAL FREE TOOLS FOR DEBUGGING WINDOWS APPLICATIONS
THESE DEBUGGING TOOLS CAN BE USED BY ANYONE BY SIMPLY DOWNLOADING THEM FROM THE INTERNET AND LEARNING HOW TO USE THEM
ALL MICROSOFT WINDOWS CLIENT AND SERVER OPERATING SYSTEM SHIP WITH AN EMBEDDED DEBUGGER
POST MORTEM DEBUGGERS
DR. WATSON
WINDOWS ERROR REPORTING (WER)
PRODUCTION DEBUGGER
AUTO DUMP PLUS (ADPLUS) – DEBUGGING TOOLS FOR WINDOWS
9

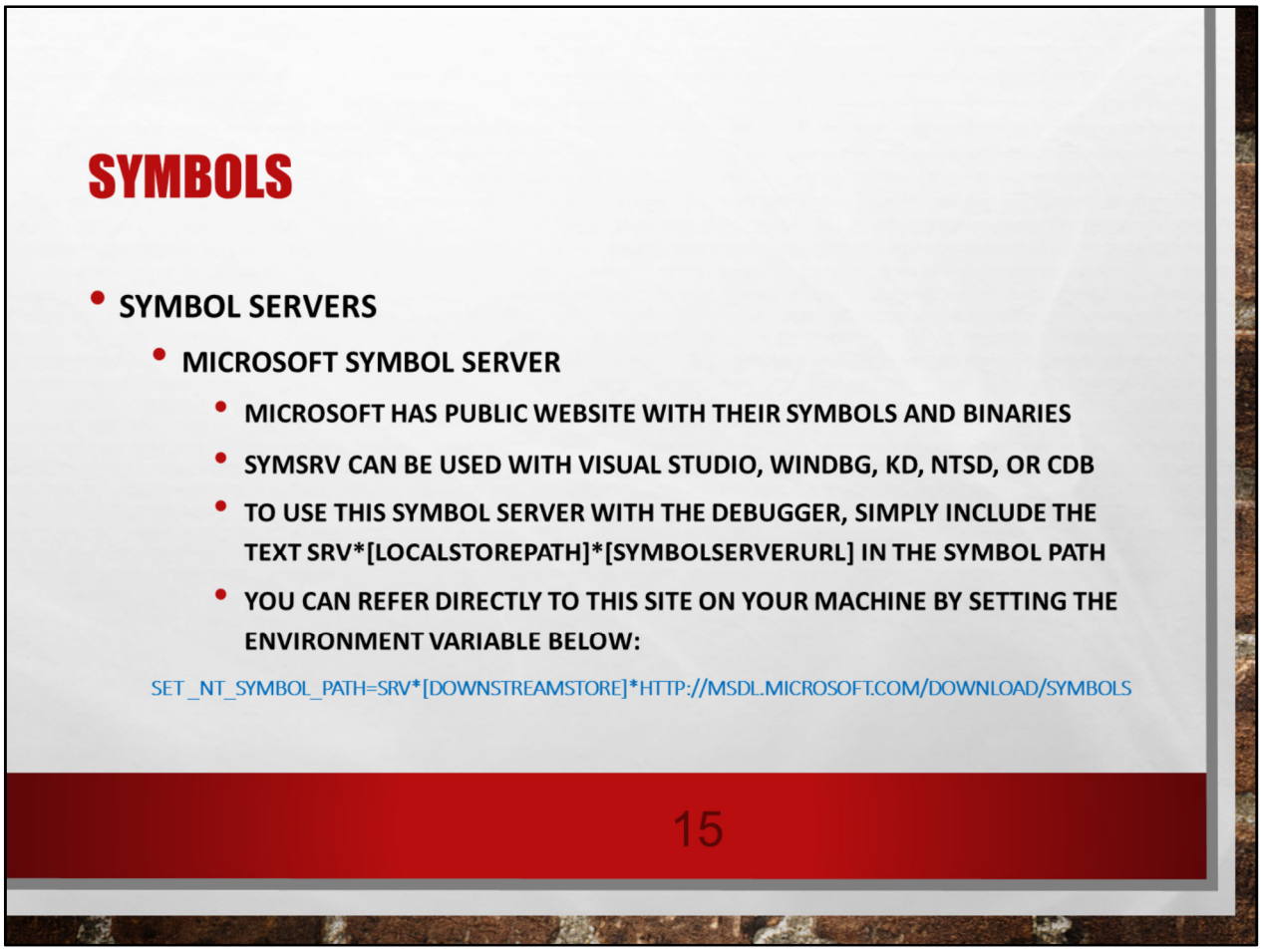

OVERVIEW
MULTIPURPOSE DEBUGGERS RECOMMENDED BY MICROSOFT
WINDOWS FORMS BASED USER MODE DEBUGGERS
VISUAL STUDIO – WINDOWS DRIVER KIT (WDK)
WINDBG – DEBUGGING TOOLS FOR WINDOWS
COMMAND LINE USER MODE DEBUGGERS
MICROSOFT CONSOLE DEBUGGER (CDB) – DEBUGGING TOOLS FOR WINDOWS
MICROSOFT SYMBOLIC DEBUGGER (NTSD) – DEBUGGING TOOLS FOR WINDOWS
COMMAND LINE KERNEL DEBUGGERS
KERNEL DEBUGGER (KD) – DEBUGGING TOOLS FOR WINDOWS
NT KERNEL DEBUGGER (NTKD) – DEBUGGING TOOLS FOR WINDOWS
10

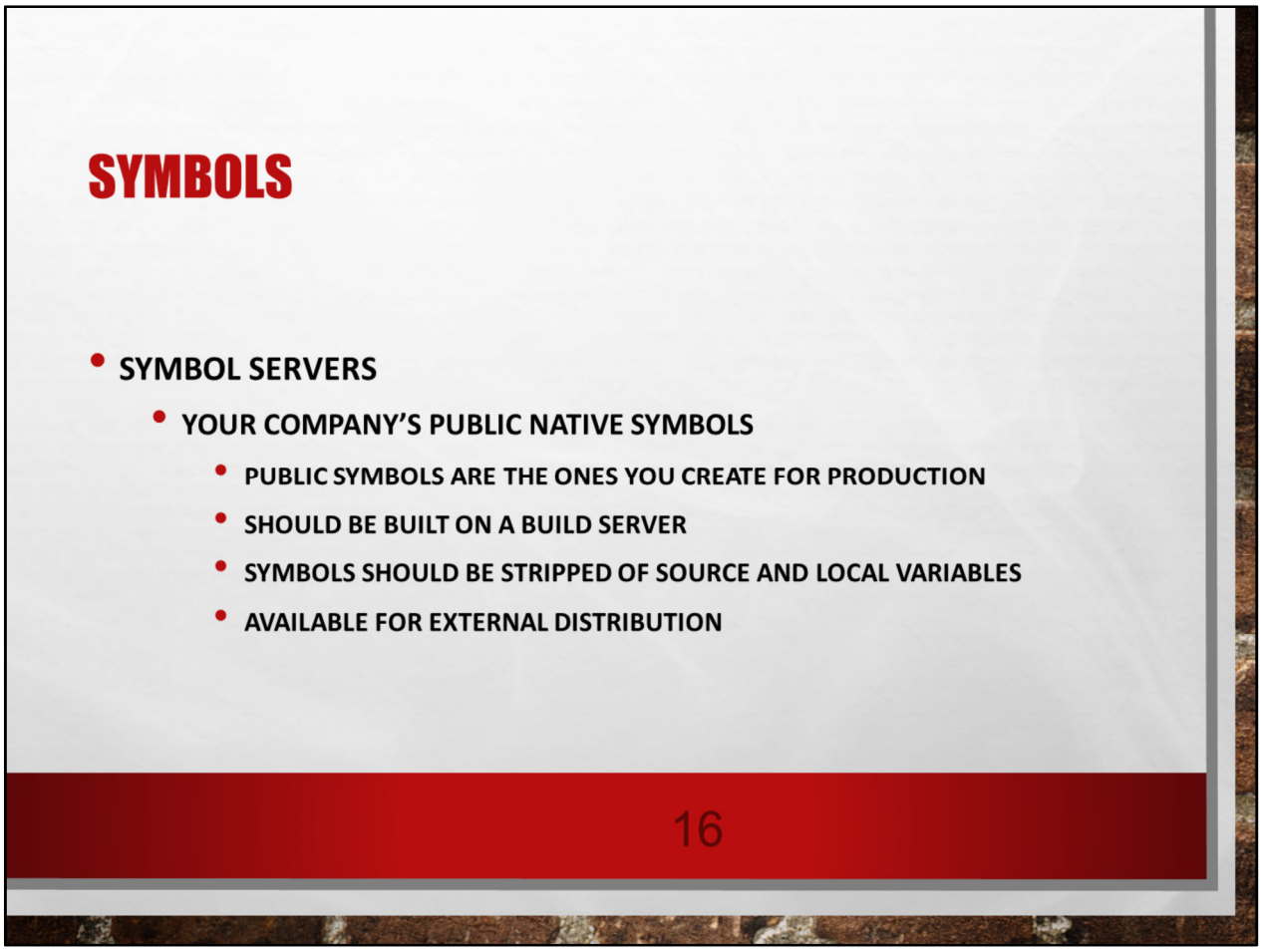

Symbols

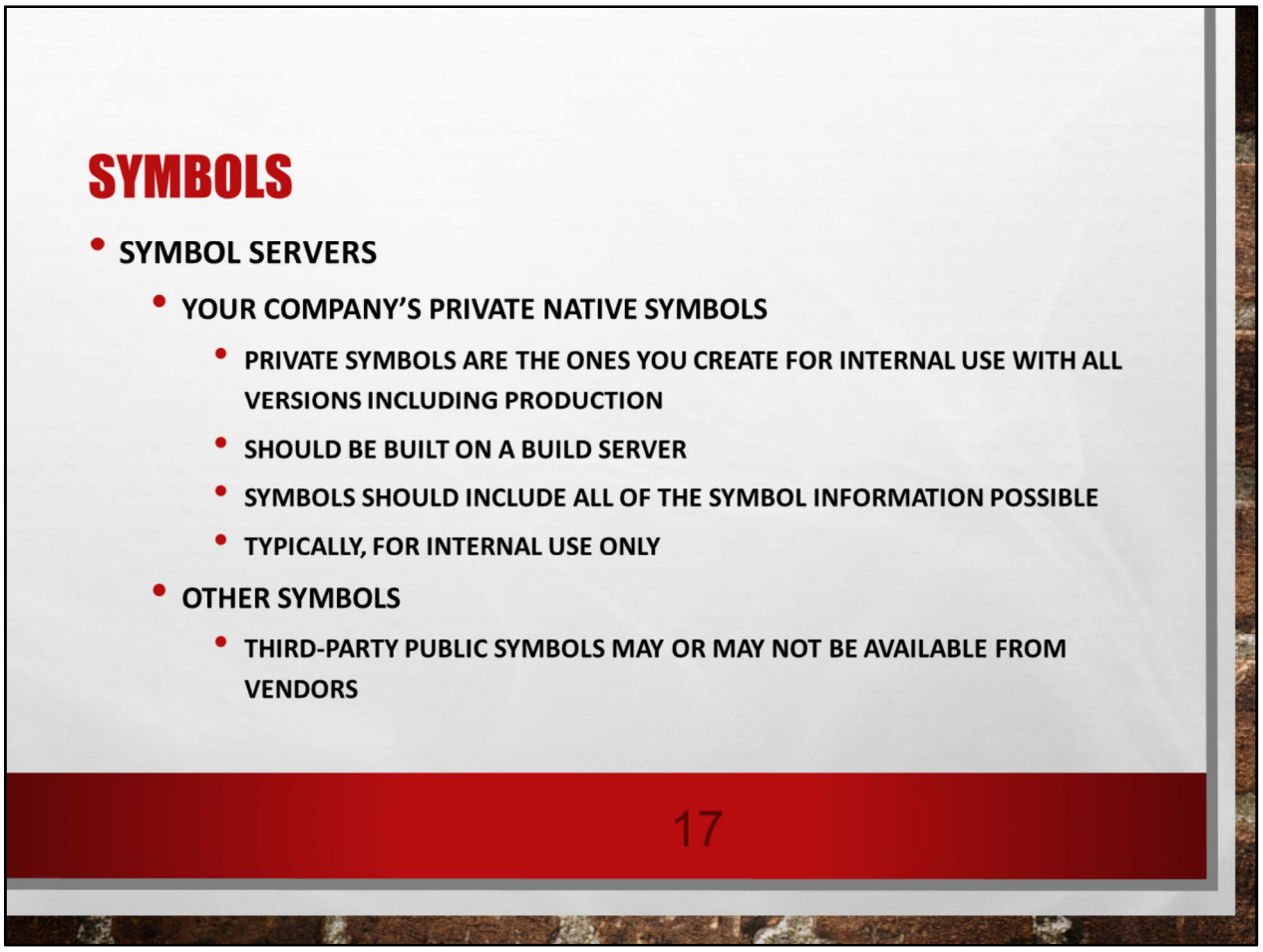

SYMBOLS
SYMBOL FILES
SYMBOLS CONTAIN A VARIETY OF DATA WHICH IS NOT NEEDED WHEN RUNNING THE BINARIES, BUT WHICH IS CRITICAL FOR DEBUGGING
NATIVE SYMBOLS
PUBLIC
PRIVATE
.NET SYMBOLS
12

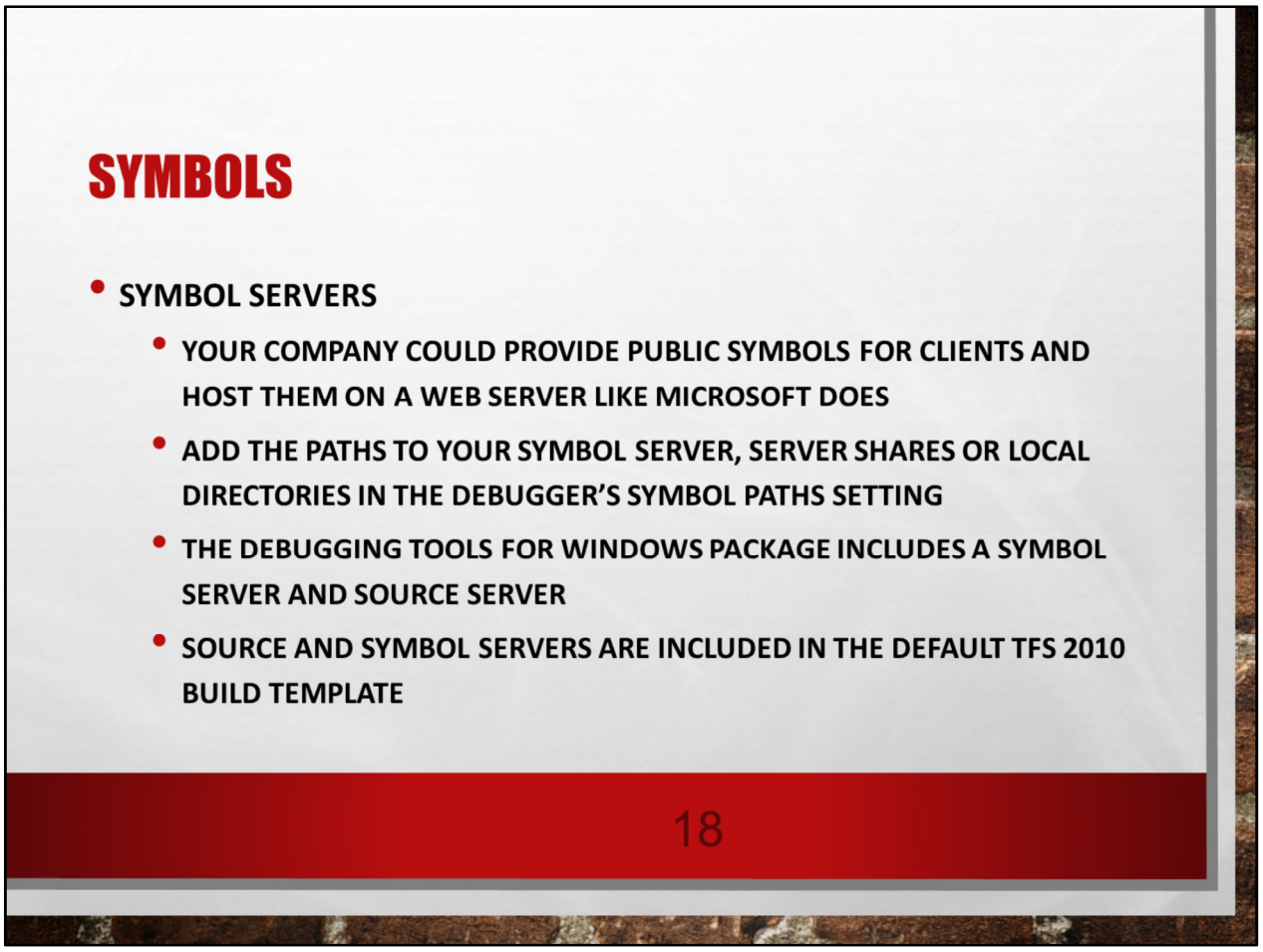

SYMBOLS
NATIVE SYMBOLS CONTENTS VARY
PRIVATE SYMBOL DATA
FUNCTIONS
GLOBAL VARIABLES
LOCAL VARIABLES
INFORMATION ABOUT USER-DEFINED STRUCTURES, CLASSES, AND DATA TYPES
THE NAME OF THE SOURCE FILE AND THE LINE NUMBER IN THAT FILE CORRESPONDING TO EACH BINARY INSTRUCTION
PUBLIC SYMBOL TABLE
FUNCTIONS AND THEIR ENTRY POINTS (EXCEPT FOR FUNCTIONS DECLARED STATIC)
GLOBAL VARIABLES SPECIFIED AS EXTERN (AND ANY OTHER GLOBAL VARIABLES VISIBLE ACROSS MULTIPLE OBJECT FILES)
13


SYMBOLS
.NET SYMBOLS
.NET SYMBOL FILES CONTAIN:
SOURCE FILE NAMES AND THEIR LINES
LOCAL VARIABLE NAMES
THERE IS NOTHING SPECIFICALLY SENSITIVE ABOUT .NET SYMBOLS
WHEN NEEDED FOR DEBUGGING, IT'S RECOMMENDED TO INSTALL .NET SYMBOL FILES SO THEY ARE IN THE SAME DIRECTORIES AS THEIR MATCHING BINARY FILE
BY HAVING THE SYMBOLS, .NET EXCEPTION CLASSES INCLUDE STACK TRACE DETAILS FOR UNHANDLED EXCEPTIONS WITH THE SOURCE AND LINE FOR EACH STACK FRAME
14


SYMBOLS
SYMBOL SERVERS
MICROSOFT SYMBOL SERVER
MICROSOFT HAS PUBLIC WEBSITE WITH THEIR SYMBOLS AND BINARIES
SYMSRV CAN BE USED WITH VISUAL STUDIO, WINDBG, KD, NTSD, OR CDB
TO USE THIS SYMBOL SERVER WITH THE DEBUGGER, SIMPLY INCLUDE THE TEXT SRV*[LOCALSTOREPATH]*[SYMBOLSERVERURL] IN THE SYMBOL PATH
YOU CAN REFER DIRECTLY TO THIS SITE ON YOUR MACHINE BY SETTING THE ENVIRONMENT VARIABLE BELOW:
SET _NT_SYMBOL_PATH=SRV*[DOWNSTREAMSTORE]*HTTP://MSDL.MICROSOFT.COM/DOWNLOAD/SYMBOLS
15

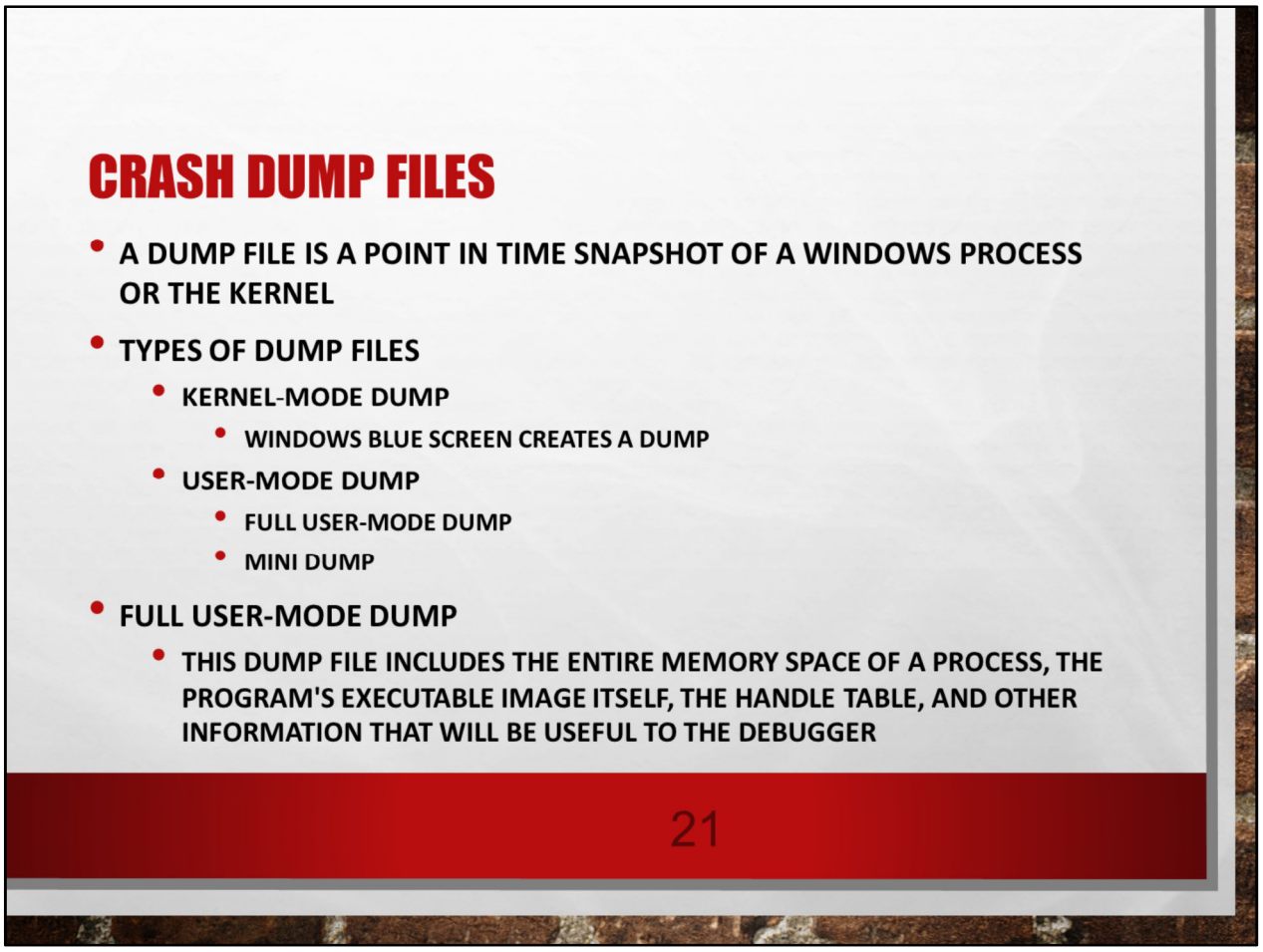

SYMBOLS
SYMBOL SERVERS
YOUR COMPANY'S PUBLIC NATIVE SYMBOLS
PUBLIC SYMBOLS ARE THE ONES YOU CREATE FOR PRODUCTION
SHOULD BE BUILT ON A BUILD SERVER
SYMBOLS SHOULD BE STRIPPED OF SOURCE AND LOCAL VARIABLES
AVAILABLE FOR EXTERNAL DISTRIBUTION
16

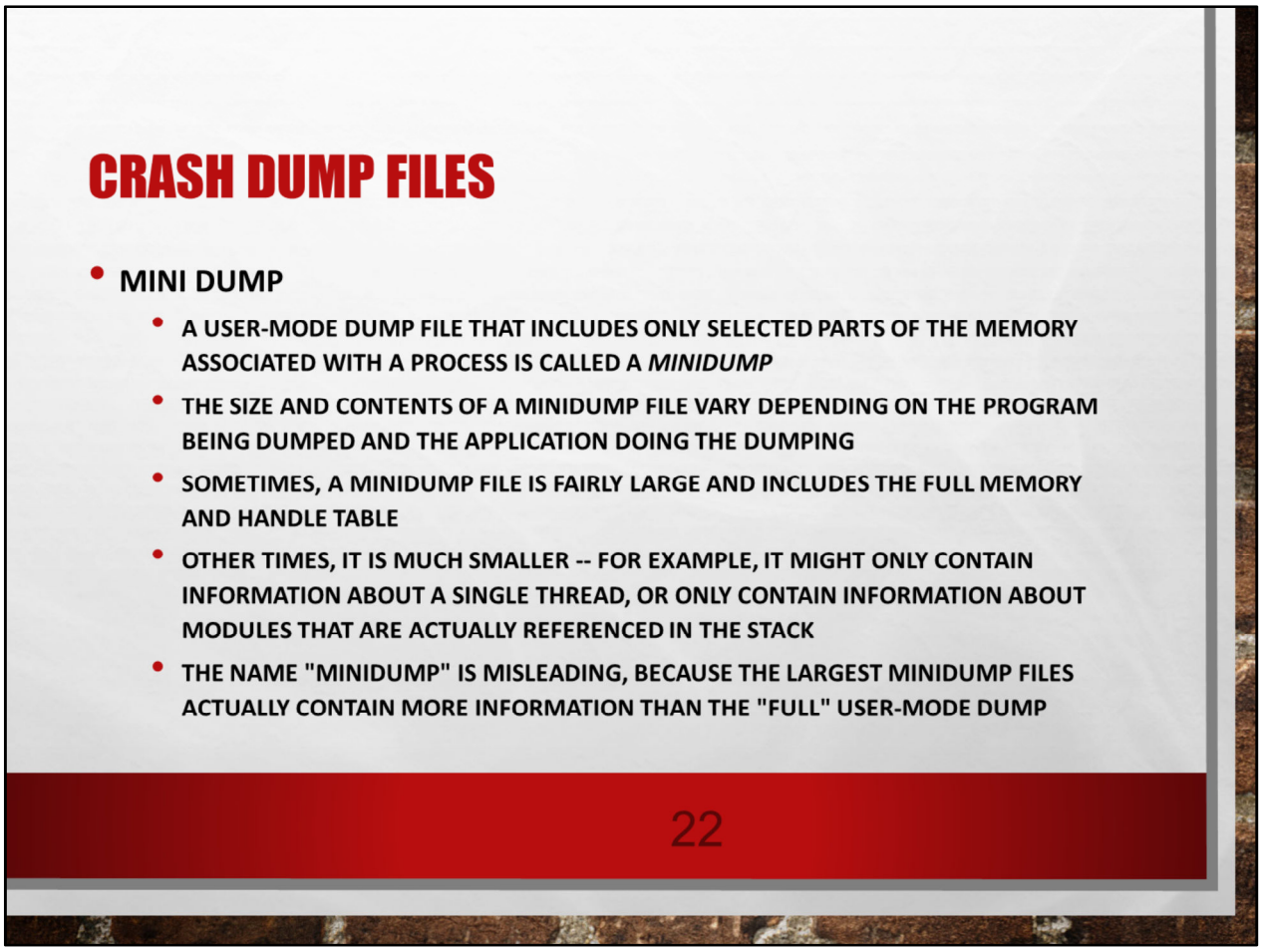

SYMBOLS
SYMBOL SERVERS
YOUR COMPANY'S PRIVATE NATIVE SYMBOLS
PRIVATE SYMBOLS ARE THE ONES YOU CREATE FOR INTERNAL USE WITH ALL VERSIONS INCLUDING PRODUCTION
SHOULD BE BUILT ON A BUILD SERVER
SYMBOLS SHOULD INCLUDE ALL OF THE SYMBOL INFORMATION POSSIBLE
TYPICALLY, FOR INTERNAL USE ONLY
OTHER SYMBOLS
THIRD-PARTY PUBLIC SYMBOLS MAY OR MAY NOT BE AVAILABLE FROM VENDORS
17

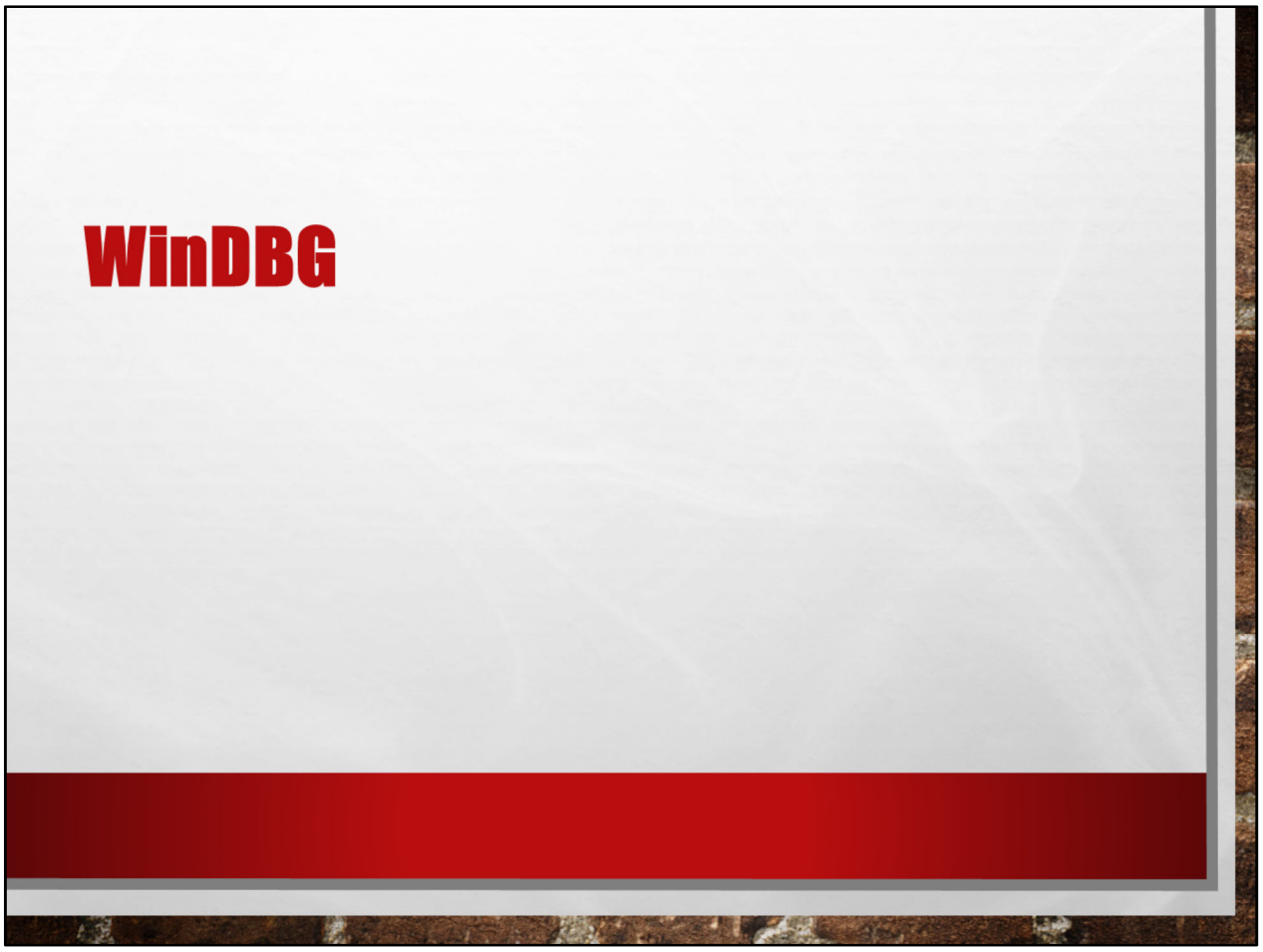

SYMBOLS
SYMBOL SERVERS
YOUR COMPANY COULD PROVIDE PUBLIC SYMBOLS FOR CLIENTS AND HOST THEM ON A WEB SERVER LIKE MICROSOFT DOES
ADD THE PATHS TO YOUR SYMBOL SERVER, SERVER SHARES OR LOCAL DIRECTORIES IN THE DEBUGGER'S SYMBOL PATHS SETTING
THE DEBUGGING TOOLS FOR WINDOWS PACKAGE INCLUDES A SYMBOL SERVER AND SOURCE SERVER
SOURCE AND SYMBOL SERVERS ARE INCLUDED IN THE DEFAULT TFS 2010 BUILD TEMPLATE
18

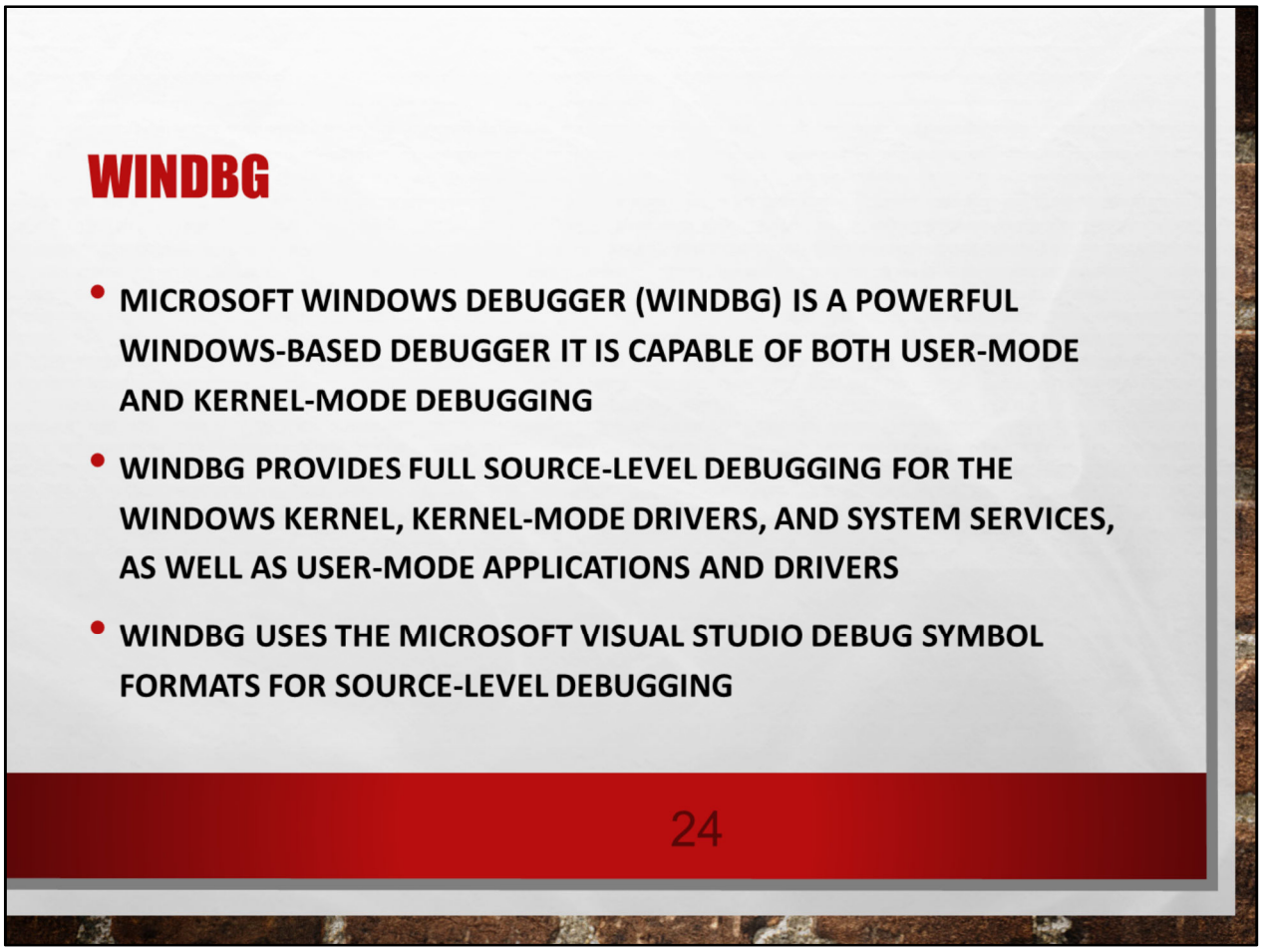

SYMBOLS
JOHN ROBINS BLOG ARTICLE - PDB FILES: WHAT EVERY DEVELOPER MUST KNOW
HTTP://WWW.WINTELLECT.COM/BLOGS/JROBBINS/PDB-FILES-WHAT-EVERY-DEVELOPER-MUST-KNOW
FOR .NET DEVELOPMENT SHOPS, WATCH OUT FOR CODE OBFUSCATION UTILITIES
YOU'LL WANT TO KEEP NORMAL AND OBFUSCATED SYMBOLS
19

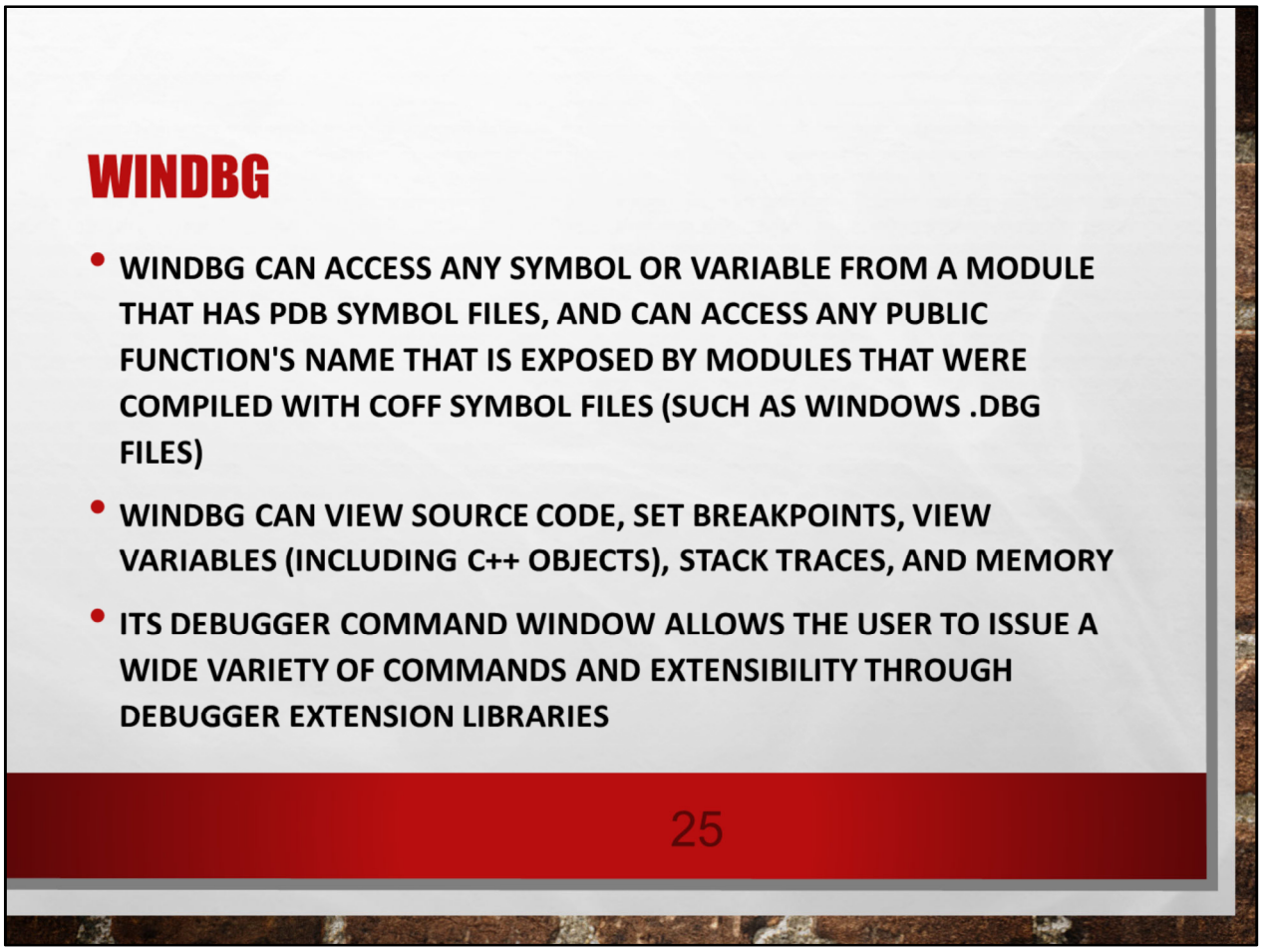

Crash Dump Files

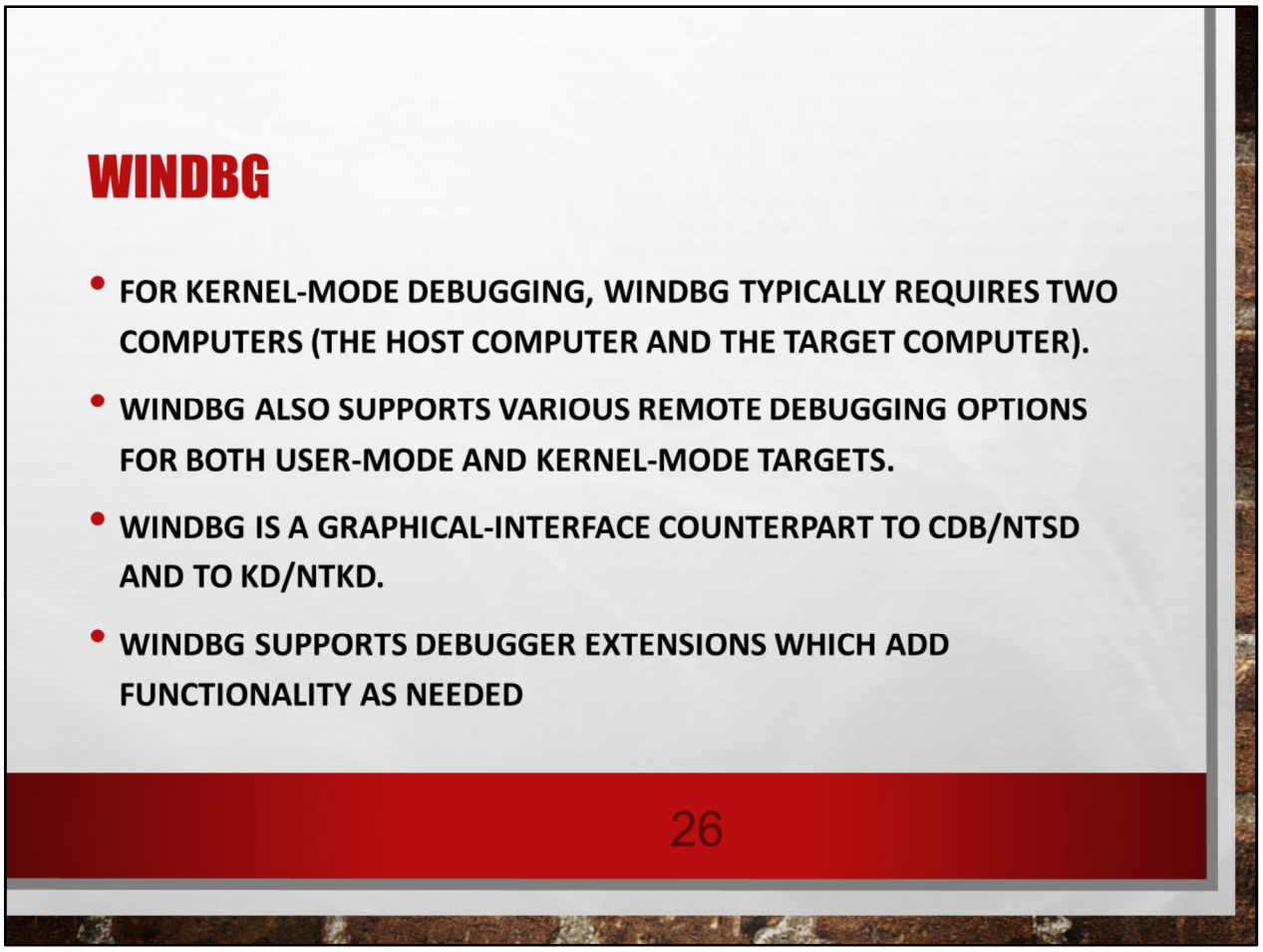

CRASH DUMP FILES
A DUMP FILE IS A POINT IN TIME SNAPSHOT OF A WINDOWS PROCESS OR THE KERNEL
TYPES OF DUMP FILES
KERNEL-MODE DUMP
WINDOWS BLUE SCREEN CREATES A DUMP
USER-MODE DUMP
FULL USER-MODE DUMP
MINI DUMP
FULL USER-MODE DUMP
THIS DUMP FILE INCLUDES THE ENTIRE MEMORY SPACE OF A PROCESS, THE PROGRAM'S EXECUTABLE IMAGE ITSELF, THE HANDLE TABLE, AND OTHER INFORMATION THAT WILL BE USEFUL TO THE DEBUGGER
21


CRASH DUMP FILES
MINI DUMP
A USER-MODE DUMP FILE THAT INCLUDES ONLY SELECTED PARTS OF THE MEMORY ASSOCIATED WITH A PROCESS IS CALLED A *MINIDUMP*
THE SIZE AND CONTENTS OF A MINIDUMP FILE VARY DEPENDING ON THE PROGRAM BEING DUMPED AND THE APPLICATION DOING THE DUMPING
SOMETIMES, A MINIDUMP FILE IS FAIRLY LARGE AND INCLUDES THE FULL MEMORY AND HANDLE TABLE
OTHER TIMES, IT IS MUCH SMALLER -- FOR EXAMPLE, IT MIGHT ONLY CONTAIN INFORMATION ABOUT A SINGLE THREAD, OR ONLY CONTAIN INFORMATION ABOUT MODULES THAT ARE ACTUALLY REFERENCED IN THE STACK
THE NAME "MINIDUMP" IS MISLEADING, BECAUSE THE LARGEST MINIDUMP FILES ACTUALLY CONTAIN MORE INFORMATION THAN THE "FULL" USER-MODE DUMP
22


WinDBG


WINDBG
MICROSOFT WINDOWS DEBUGGER (WINDBG) IS A POWERFUL WINDOWS-BASED DEBUGGER IT IS CAPABLE OF BOTH USER-MODE AND KERNEL-MODE DEBUGGING
WINDBG PROVIDES FULL SOURCE-LEVEL DEBUGGING FOR THE WINDOWS KERNEL, KERNEL-MODE DRIVERS, AND SYSTEM SERVICES, AS WELL AS USER-MODE APPLICATIONS AND DRIVERS
WINDBG USES THE MICROSOFT VISUAL STUDIO DEBUG SYMBOL FORMATS FOR SOURCE-LEVEL DEBUGGING
24

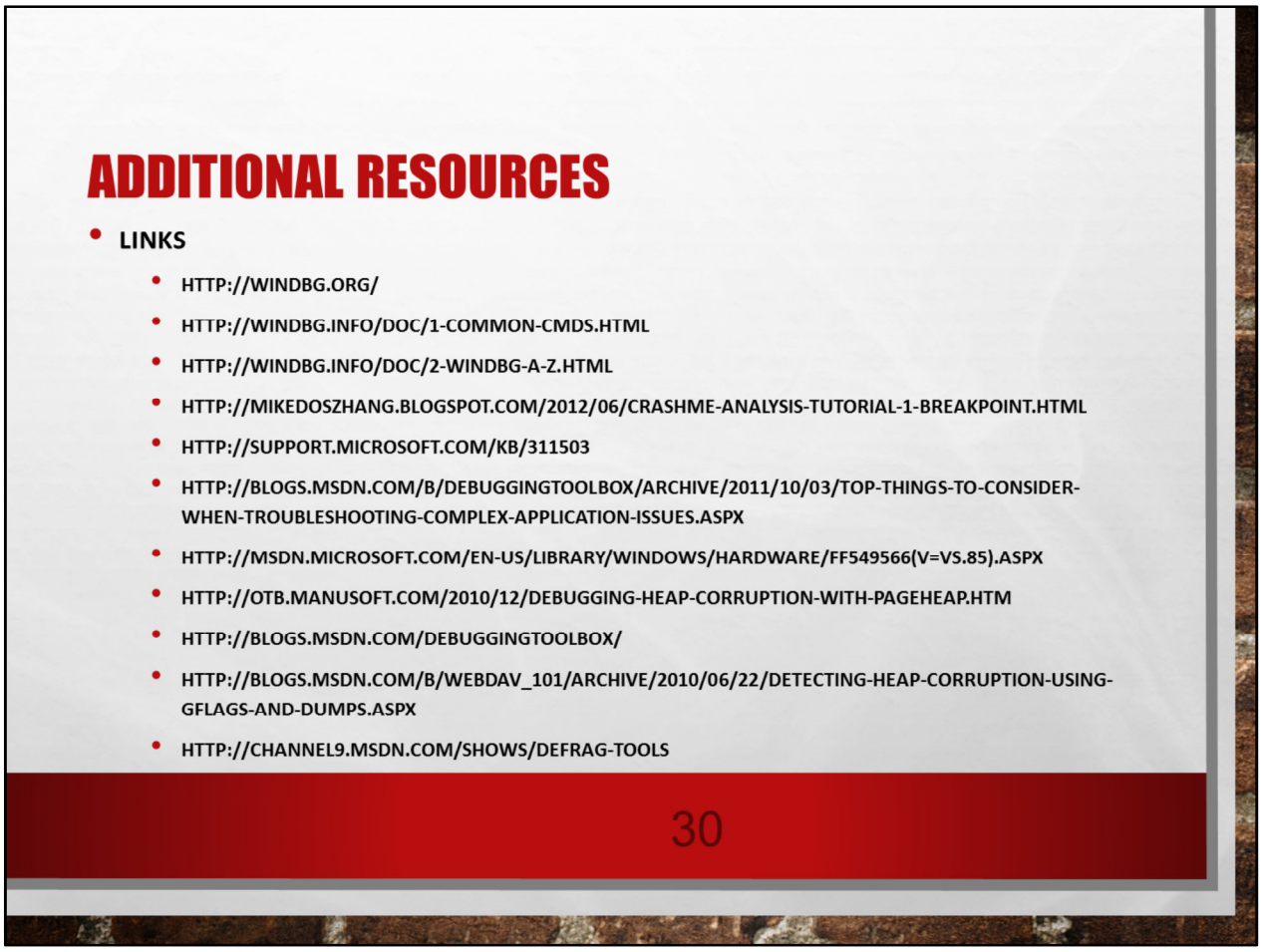

WINDBG
WINDBG CAN ACCESS ANY SYMBOL OR VARIABLE FROM A MODULE THAT HAS PDB SYMBOL FILES, AND CAN ACCESS ANY PUBLIC FUNCTION'S NAME THAT IS EXPOSED BY MODULES THAT WERE COMPILED WITH COFF SYMBOL FILES (SUCH AS WINDOWS .DBG FILES)
WINDBG CAN VIEW SOURCE CODE, SET BREAKPOINTS, VIEW VARIABLES (INCLUDING C++ OBJECTS), STACK TRACES, AND MEMORY
ITS DEBUGGER COMMAND WINDOW ALLOWS THE USER TO ISSUE A WIDE VARIETY OF COMMANDS AND EXTENSIBILITY THROUGH DEBUGGER EXTENSION LIBRARIES
25

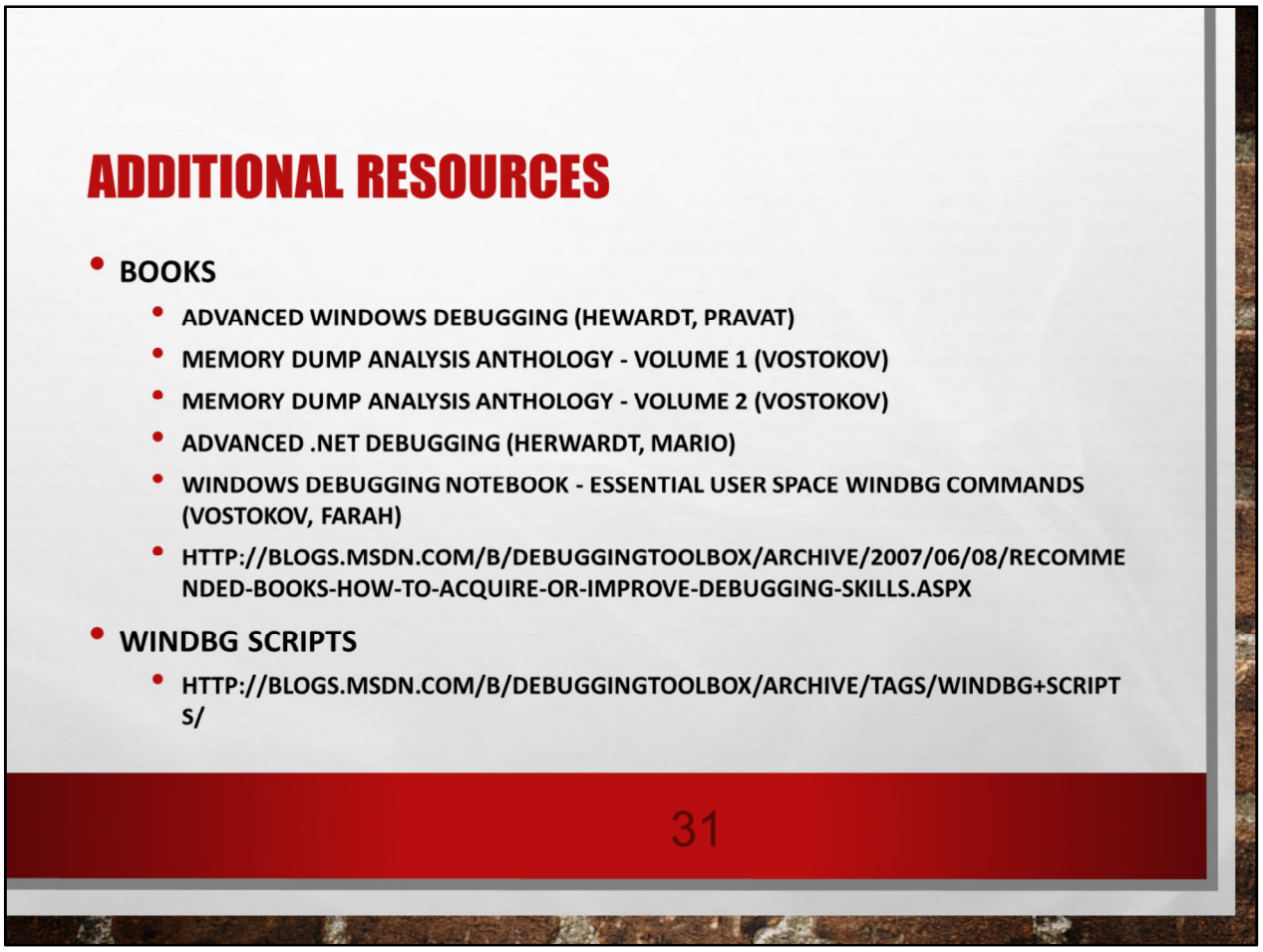

WINDBG
FOR KERNEL-MODE DEBUGGING, WINDBG TYPICALLY REQUIRES TWO COMPUTERS (THE HOST COMPUTER AND THE TARGET COMPUTER).
WINDBG ALSO SUPPORTS VARIOUS REMOTE DEBUGGING OPTIONS FOR BOTH USER-MODE AND KERNEL-MODE TARGETS.
WINDBG IS A GRAPHICAL-INTERFACE COUNTERPART TO CDB/NTSD AND TO KD/NTKD.
WINDBG SUPPORTS DEBUGGER EXTENSIONS WHICH ADD FUNCTIONALITY AS NEEDED
26

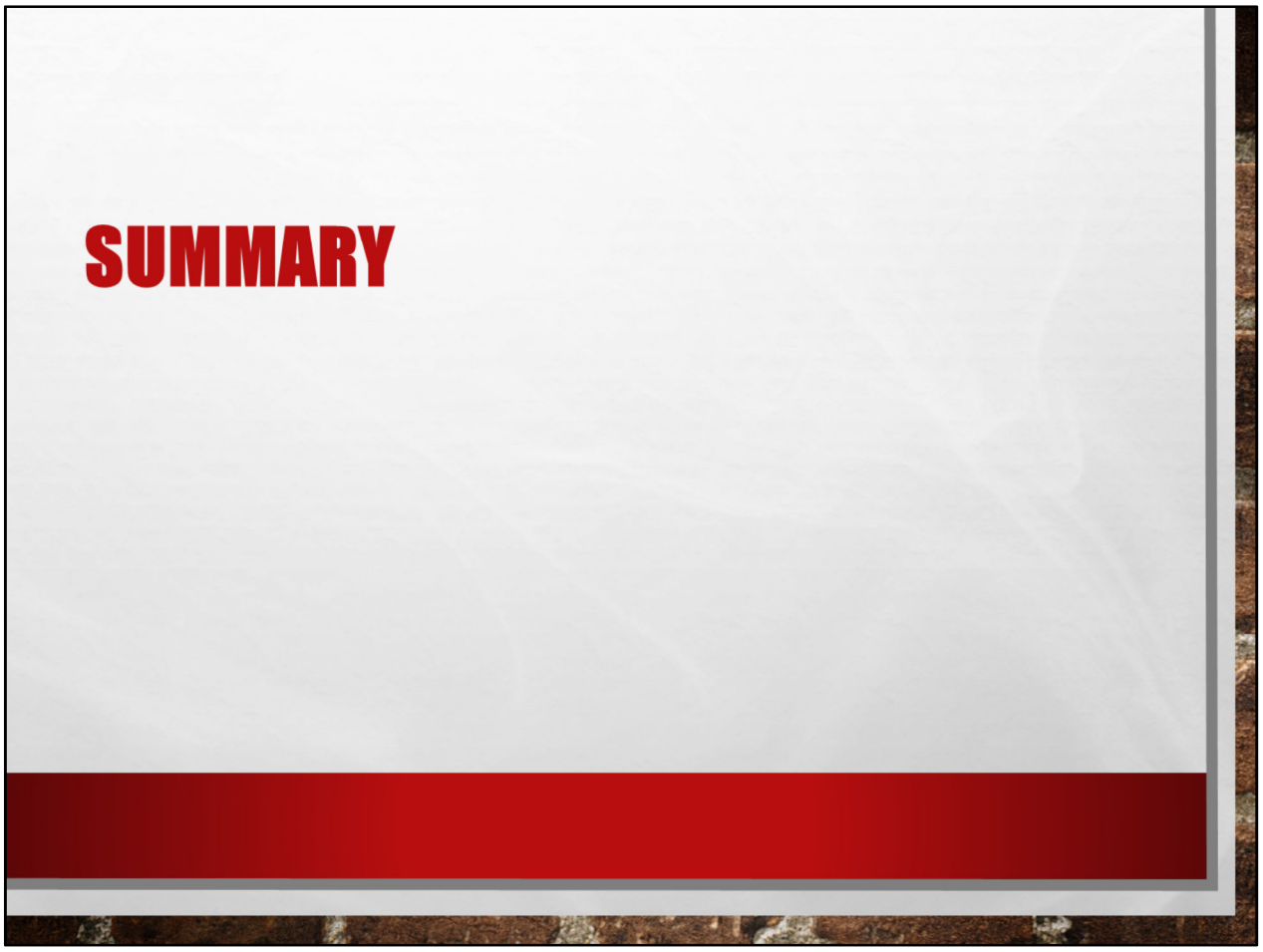

WINDBG
EXTENSIONS
SOS – THE .NET FRAMEWORK EXTENSION (VERSION-SPECIFIC)
INSTALLED WITH THE .NET FRAMEWORK
PSSCOR4 – MICROSOFT PREMIER SUPPORT VERSIONS OF SOS
HTTP://WWW.MICROSOFT.COM/EN-US/DOWNLOAD/DETAILS.ASPX?ID=21255
SOSEX – "A DEBUGGING EXTENSION FOR MANAGED CODE THAT BEGINS TO ALLEVIATE SOME OF MY FRUSTRATIONS WITH SOS"
HTTP://WWW.STEVESTECHSPOT.COM/DEFAULT.ASPX
SPT – "AUTOMATES COMMON .NET DEBUGGING TASKS"
HTTP://BLOG.STEVENIEMITZ.COM/PAGE/2/
27

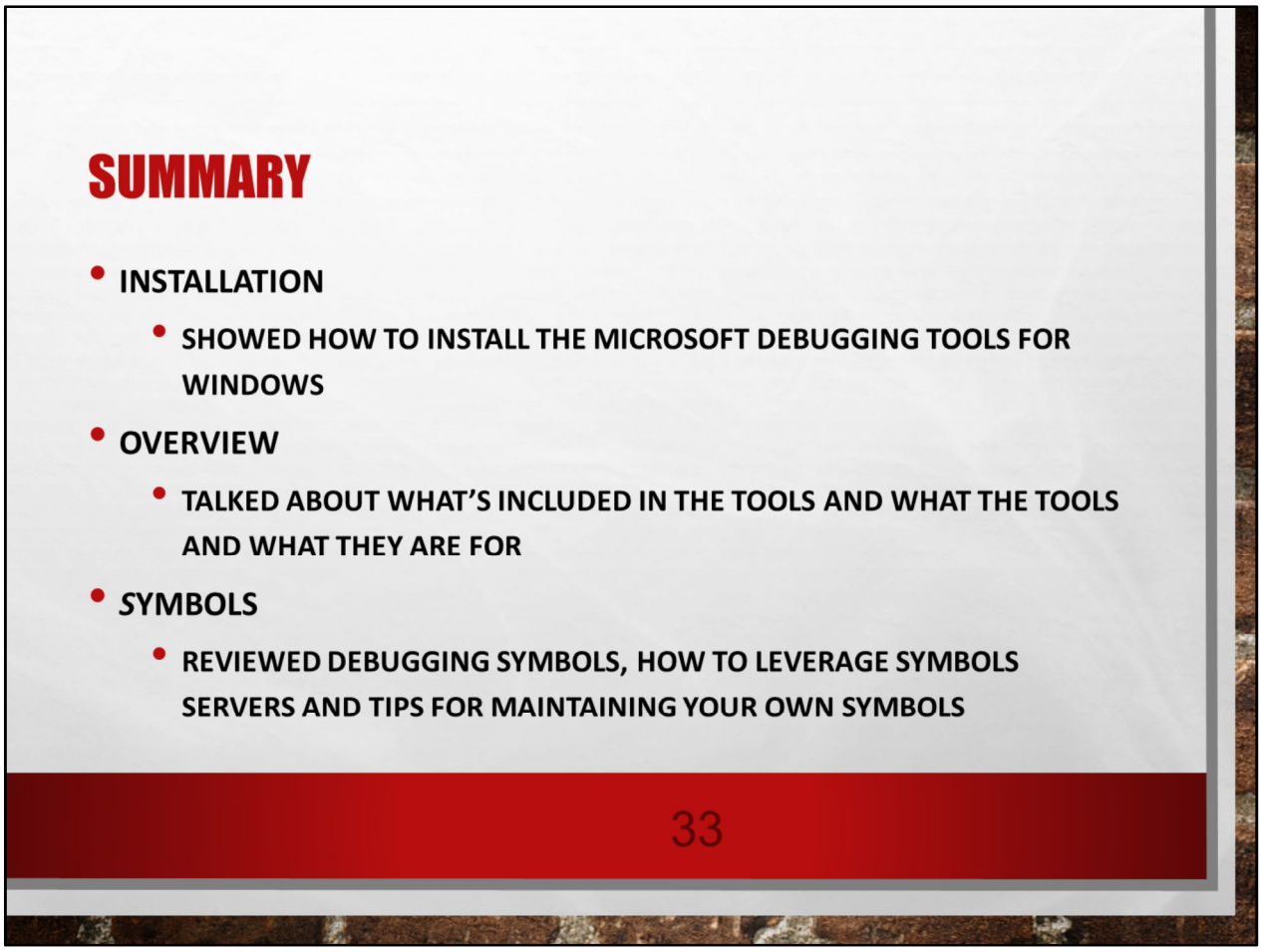

Demo

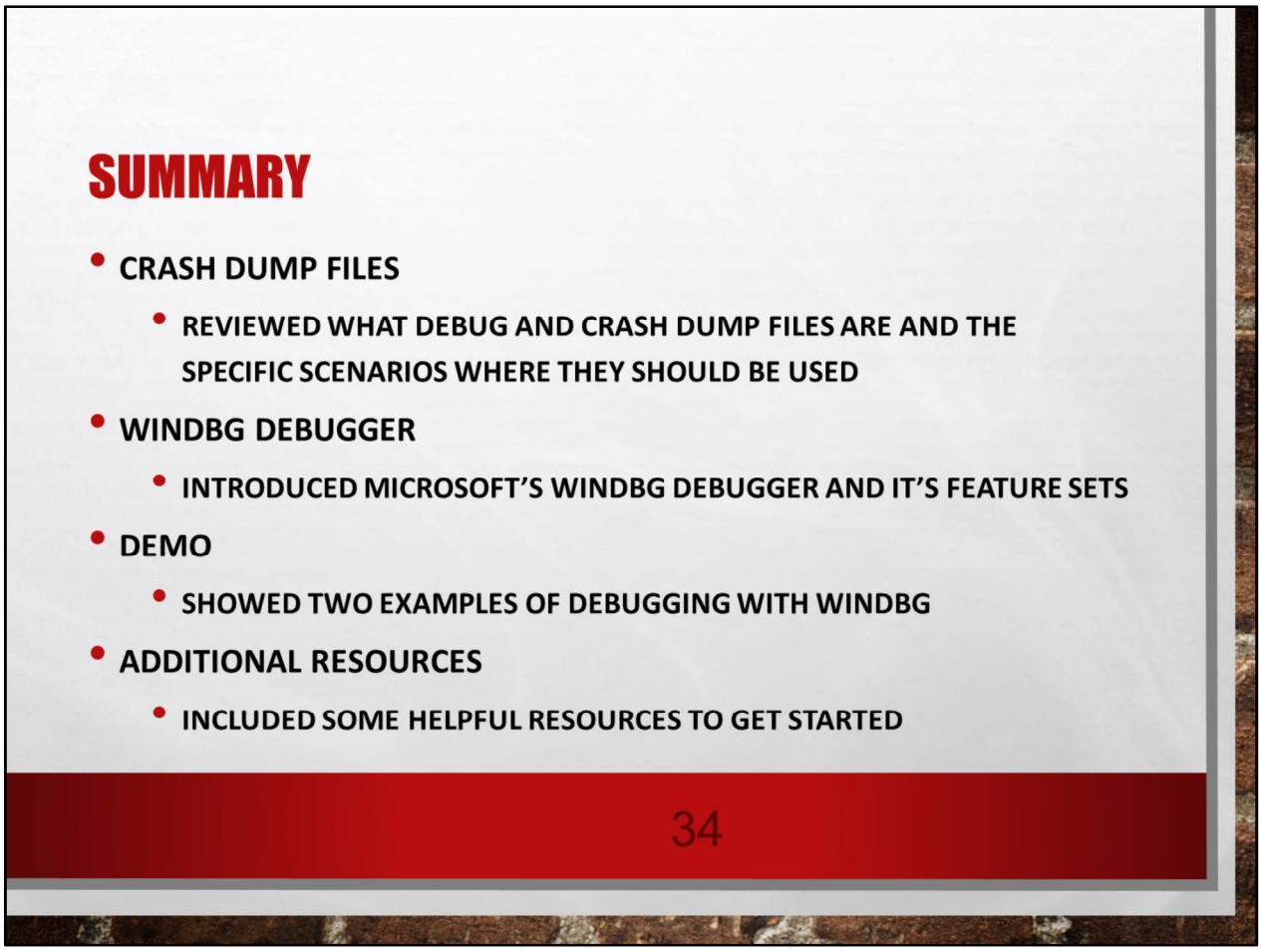

Additional Resources


ADDITIONAL RESOURCES
LINKS
HTTP://WINDBG.ORG/
HTTP://WINDBG.INFO/DOC/1-COMMON-CMDS.HTML
HTTP://WINDBG.INFO/DOC/2-WINDBG-A-Z.HTML
HTTP://MIKEDOSZHANG.BLOGSPOT.COM/2012/06/CRASHME-ANALYSIS-TUTORIAL-1-BREAKPOINT.HTML
HTTP://SUPPORT.MICROSOFT.COM/KB/311503
HTTP://BLOGS.MSDN.COM/B/DEBUGGINGTOOLBOX/ARCHIVE/2011/10/03/TOP-THINGS-TO-CONSIDER-WHEN-TROUBLESHOOTING-COMPLEX-APPLICATION-ISSUES.ASPX
HTTP://MSDN.MICROSOFT.COM/EN-US/LIBRARY/WINDOWS/HARDWARE/FF549566(V=VS.85).ASPX
HTTP://OTB.MANUSOFT.COM/2010/12/DEBUGGING-HEAP-CORRUPTION-WITH-PAGEHEAP.HTM
HTTP://BLOGS.MSDN.COM/DEBUGGINGTOOLBOX/
HTTP://BLOGS.MSDN.COM/B/WEBDAV_101/ARCHIVE/2010/06/22/DETECTING-HEAP-CORRUPTION-USING-GFLAGS-AND-DUMPS.ASPX
HTTP://CHANNEL9.MSDN.COM/SHOWS/DEFRAG-TOOLS
30

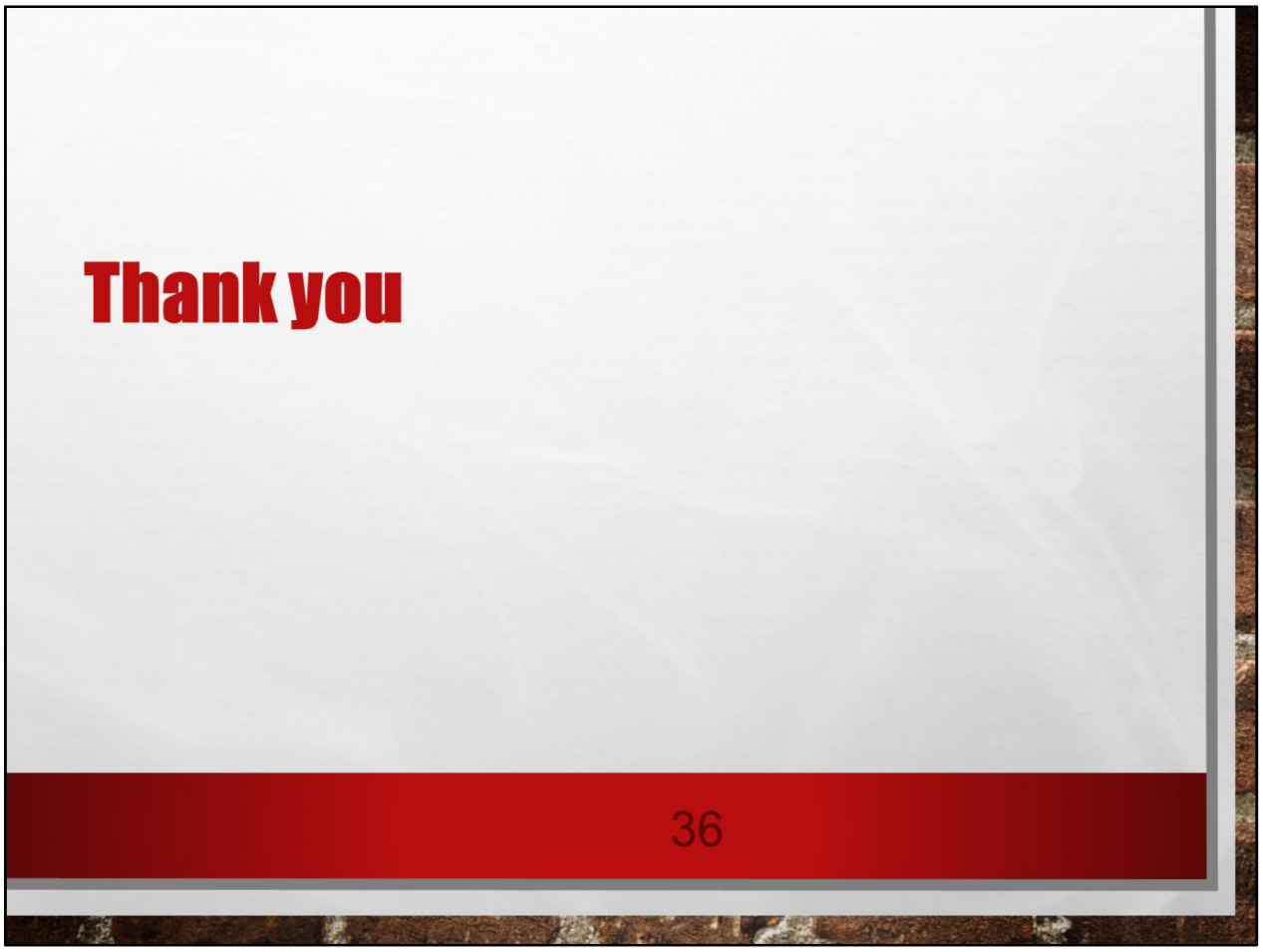

ADDITIONAL RESOURCES
BOOKS
ADVANCED WINDOWS DEBUGGING (HEWARDT, PRAVAT)
MEMORY DUMP ANALYSIS ANTHOLOGY - VOLUME 1 (VOSTOKOV)
MEMORY DUMP ANALYSIS ANTHOLOGY - VOLUME 2 (VOSTOKOV)
ADVANCED .NET DEBUGGING (HERWARDT, MARIO)
WINDOWS DEBUGGING NOTEBOOK - ESSENTIAL USER SPACE WINDBG COMMANDS (VOSTOKOV, FARAH)
HTTP://BLOGS.MSDN.COM/B/DEBUGGINGTOOLBOX/ARCHIVE/2007/06/08/RECOMMENDED-BOOKS-HOW-TO-ACQUIRE-OR-IMPROVE-DEBUGGING-SKILLS.ASPX
WINDBG SCRIPTS
HTTP://BLOGS.MSDN.COM/B/DEBUGGINGTOOLBOX/ARCHIVE/TAGS/WINDBG+SCRIPTS/
31


SUMMARY


SUMMARY
INSTALLATION
SHOWED HOW TO INSTALL THE MICROSOFT DEBUGGING TOOLS FOR WINDOWS
OVERVIEW
TALKED ABOUT WHAT'S INCLUDED IN THE TOOLS AND WHAT THE TOOLS AND WHAT THEY ARE FOR
SYMBOLS
REVIEWED DEBUGGING SYMBOLS, HOW TO LEVERAGE SYMBOLS SERVERS AND TIPS FOR MAINTAINING YOUR OWN SYMBOLS
33


SUMMARY
CRASH DUMP FILES
REVIEWED WHAT DEBUG AND CRASH DUMP FILES ARE AND THE SPECIFIC SCENARIOS WHERE THEY SHOULD BE USED
WINDBG DEBUGGER
INTRODUCED MICROSOFT'S WINDBG DEBUGGER AND IT'S FEATURE SETS
DEMO
SHOWED TWO EXAMPLES OF DEBUGGING WITH WINDBG
ADDITIONAL RESOURCES
INCLUDED SOME HELPFUL RESOURCES TO GET STARTED
34


Q&A
35


Thank you
36


James Stephenson
jamesgstephenson@gmail.com
https://www.linkedin.com/in/jamesgstephenson
https://twitter.com/JStephensonFL
37