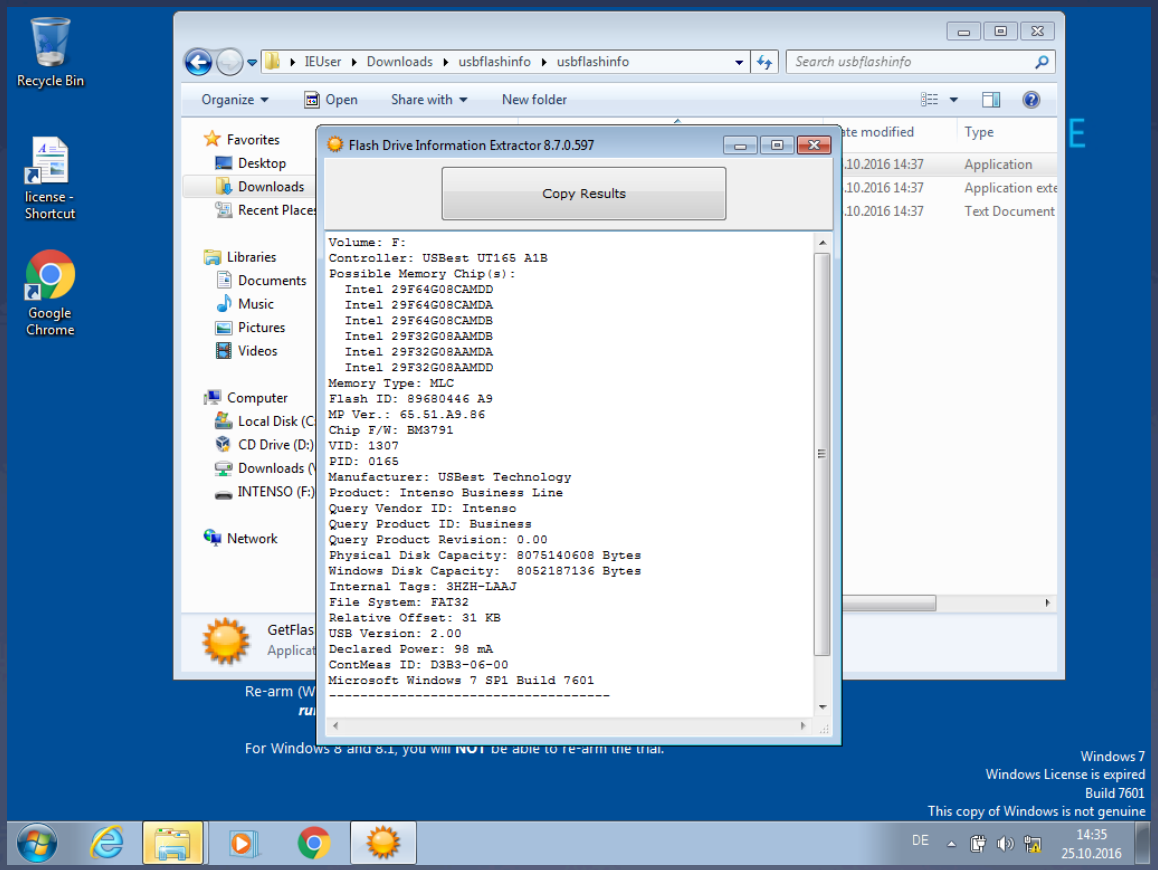
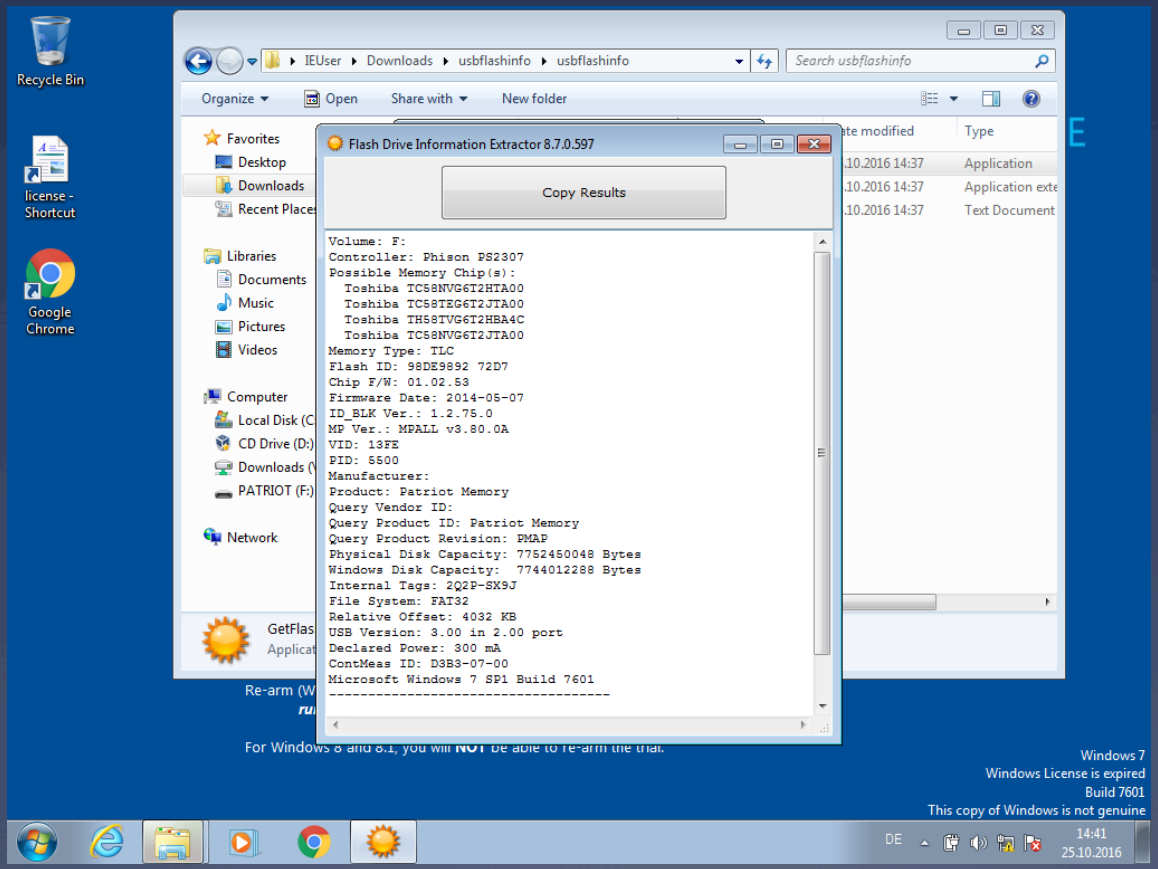
Bad USB

6. Security Meetup
Kassel, Matthias Altmann

Bad USB

* https://srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf
* https://github.com/daveti/badusb/blob/master/ppt/SRLabs-BadUSB-Pacsec-v2.pdf
* https://github.com/brandonlw/Psychson
* https://opensource.srlabs.de/projects/badusb
* http://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/
* https://www.pjrc.com/teensy/


Recycle Bin
license - Shortcut
Google Chrome
IEUser ▸ Downloads ▸ usbflashinfo ▸ usbflashinfo
Search usbflashinfo
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C
CD Drive (D:)
Downloads (\
INTENSO (F:)
Network
Type
.10.2016 14:37 Application
.10.2016 14:37 Application exte
.10.2016 14:37 Text Document
Flash Drive Information Extractor 8.7.0.597
Copy Results
Volume: F:
Controller: USBest UT165 A1B
Possible Memory Chip(s):
Intel 29F64G08CAMDD
Intel 29F64G08CAMDA
Intel 29F64G08CAMDB
Intel 29F32G08AAMDB
Intel 29F32G08AAMDA
Intel 29F32G08AAMDD
Memory Type: MLC
Flash ID: 89680446 A9
MP Ver.: 65.51.A9.86
Chip F/W: BM3791
VID: 1307
PID: 0165
Manufacturer: USBest Technology
Product: Intenso Business Line
Query Vendor ID: Intenso
Query Product ID: Business
Query Product Revision: 0.00
Physical Disk Capacity: 8075140608 Bytes
Windows Disk Capacity: 8052187136 Bytes
Internal Tags: 3HZH-LAAJ
File System: FAT32
Relative Offset: 31 KB
USB Version: 2.00
Declared Power: 98 mA
ContMeas ID: D3B3-06-00
Microsoft Windows 7 SP1 Build 7601
GetFlas
Re-arm (W
For Windows 8 and 8.1, you will NOT be able to re-arm the trial.
Windows 7
Windows License is expired
Build 7601
This copy of Windows is not genuine
DE
14:35
25.10.2016


Recycle Bin
license - Shortcut
Google Chrome
IEUser ▸ Downloads ▸ usbflashinfo ▸ usbflashinfo
Search usbflashinfo
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C
CD Drive (D:)
Downloads (\
PATRIOT (F:)
Network
Type
.10.2016 14:37 Application
.10.2016 14:37 Application exte
.10.2016 14:37 Text Document
Flash Drive Information Extractor 8.7.0.597
Copy Results
Volume: F:
Controller: Phison PS2307
Possible Memory Chip(s):
Toshiba TC58NVG6T2HTA00
Toshiba TC58TEG6T2JTA00
Toshiba TH58TVG6T2HBA4C
Toshiba TC58NVG6T2JTA00
Memory Type: TLC
Flash ID: 98DE9892 72D7
Chip F/W: 01.02.53
Firmware Date: 2014-05-07
ID_BLK Ver.: 1.2.75.0
MP Ver.: MPALL v3.80.0A
VID: 13FE
PID: 5500
Manufacturer:
Product: Patriot Memory
Query Vendor ID:
Query Product ID: Patriot Memory
Query Product Revision: PMAP
Physical Disk Capacity: 7752450048 Bytes
Windows Disk Capacity: 7744012288 Bytes
Internal Tags: 2Q2P-SX9J
File System: FAT32
Relative Offset: 4032 KB
USB Version: 3.00 in 2.00 port
Declared Power: 300 mA
ContMeas ID: D3B3-07-00
Microsoft Windows 7 SP1 Build 7601
GetFlas
Re-arm (W
For Windows 8 and 8.1, you will NOT be able to re-arm the trial.
Windows 7
Windows License is expired
Build 7601
This copy of Windows is not genuine
DE
14:41
25.10.2016

Rubber Ducky

* https://ducktoolkit.com/
* https://github.com/hak5darren/USB-Rubber-Ducky/wiki
* Powershell Empire Rubber Ducky Modul
* https://www.powershellempire.com/?page_id=104
* Community Payload Generators, Firmware, Encoder und Toolkits
* http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe

Duckuino

* https://d4n5h.github.io/Duckuino/
* https://github.com/d4n5h/Duckuino

Encoder / Decoder

* Jar entpacken und Decompiler verwenden
* Encoder kann RTF und normalen Text
* keyboard.properties liegt Char To Hex
* Encoder#encodeToFile

Firmware

* https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Flashing-ducky

* https://forums.hak5.org/index.php?/topic/28824-faq-frequently-asked-questions/

Firmware bearbeiten

* USB-Rubber-Ducky/Firmware

VID / PID

* system_profiler SPUSBDataType
* Product ID / Vendor ID
* VID PID Swapper

Teensy

* https://www.pjrc.com/teensy/

Schutz

Hardware:

* http://www.ironkey.com/en-US/solutions/protect-against-badusb.html
* http://int3.cc/products/usbcondoms

Software:

* Keine neuen HIDs erlauben:
  http://security.stackexchange.com/questions/64524/how-to-prevent-badusb-attacks-on-linux-desktop
* Blacklisting VID/PID (Black Hat: Blacklistanalyse verkaufter Software)
  http://security.stackexchange.com/questions/92131/hardware-devices-for-protecting-against-badusb

  https://www.gdata.de/de-usb-keyboard-guard
* Scannen der USB-Firmware (Black Hat: Spoofen entsprechender Firmware)

Schutz

Organisatorisch

* USB-Sticks nicht als Übertragungsmedium verwenden
* Bildschirm sperren
* Rechner soweit möglich niemanden anderem zugänglich machen