Part 3
Windows Memory Forensics

Peter Haag
Adrian Leuenberger

Memory Forensics

Memory Forensics

Agenda:

- Live Forensics
- The Theory
- Data Acquisition
- Data Analysis
- HandsOn/Practice

Memory Forensics

Theory ... Again ...

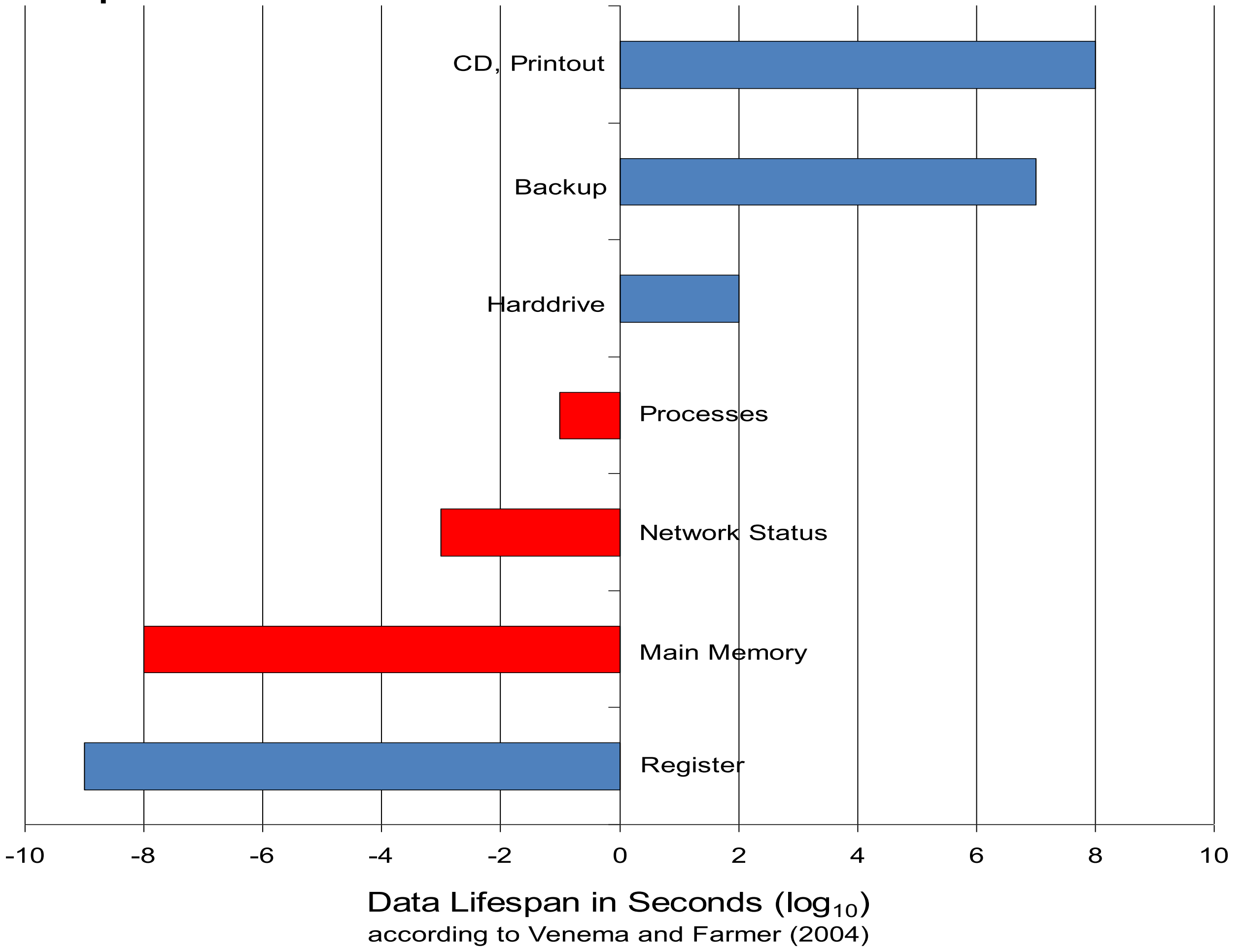
Memory Forensics

Live/Memory Forensics

- Makes data available, residing in memory which will get lost when power is switched off. (Volatile Forensics)
- Often used in incident handling, if malware is involved.
- Does not replace traditional disk forensics, but complements the methods to understand the state of a PC.
- Can be difficult as we find ourselves in an untrusted or hostile environment.
  $\Rightarrow$ Open heart surgery.
- Finally may or may not result in a full traditional disk forensic analysis depending on the findings.
- Legal aspects: Observe the law.

Memory Forensics

- Data Lifespan



Memory Forensics

Heisenberg Uncertainty Principle:
If you know where a particle is you can’t measure its speed with precision (and vice versa) without altering it!

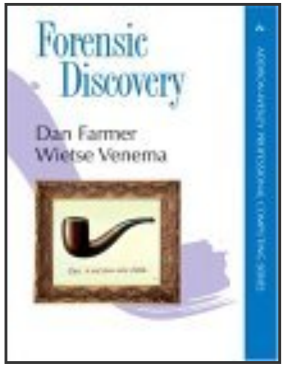
$$\Delta E \cdot \Delta t \geq \frac{h}{4\pi}$$

Forensic analysis dilemma:
Tools run in memory!
Any attempt to capture data precisely will most likely alter it!

Memory Forensics

Best Practice: Collection of data in the "order of volatility"

- 2002: RFC 3227
  Guidelines for Evidence Collection and Archiving



Forensic Discovery

Dan Farmer
Wietse Venema

- 2004: Dan Farmer and Wietse Venema
  Forensic Discovery

- 2006: NIST Special Publication 800-86
  Guide to Integrating Forensic Techniques into Incident Response

Memory Forensics

What is the proper order of volatility?

RFC 3227

- Registers, cache
- Network status
- Process information
- Main memory
- Temporary file systems
- Disk
- Remote logging and monitoring data that is relevant to the system in question
- Physical configuration, network topology
- Archival media

Forensic Discovery

- Registers, peripheral memory, caches, etc.
- Main memory
- Network status
- Process information
- Disk
- Floppies, backup media, etc.
- CD-ROMs, printouts, etc.

NIST SP 800-86

- Network status
- Login sessions
- Main memory
- Process information
- Open files
- Network configuration
- Operating system time

Memory Forensics

The basic recipe to collect live information:

- Make notes about everything which you think is important.
- Note the date and time when you start.
- Take a picture of the screen if possible. (Mobile - or Digicams)
- Take a memory image. e.g. windd.(Volatile information first)
- Run some information gathering apps such as
  - SysInternals Process Explorer
  - SysInternals Autorun
  - Winaudit
- Optionally copy suspect files and the Registry Files to a USB stick.
- Run additional AV scanner / Rootkit detectors such as
  - F-Secure Blacklight
  - GMER
- Secunia PSI (online or installed)
- Put all collected data on RO media (e.g. DVD)
- Do the memory image analysis offline.

Memory Forensics

Acquiring the memory image

- In theory there are several possibilities to acquire memory data:

Software	Hardware
• Affects CPU, memory, kernel and drivers. • Costs mainly driven by license. • Easy to deploy and maintain in a corporate environment; remotely accessible. • Can easily be fooled: “The one who installs earlier/hooks deeper, wins.”	• Low effect on CPU. • Usually requires extra hardware, FireWire may be an exception. • Installation may require significant time (more costs) and local access. • Trusted access to memory? Rutkowska attack on DMA

Memory Forensics

Caveats:

- Some tools may require admin privileges to install and would need to reboot.
- Hardware devices are often impractical to attach (except firewire)
- Some tools have an overlarge memory footprint, tampers with evidence.

“Blurred” versus “crisp” memory image:

Memory Forensics

Wishful thinking:

“crisp” memory images without tampering with anything

In theory - yes - but …
… often difficult to achieve

Memory Forensics

- Software to acquire a memory image:
  - Plenty of tools available. Most for $$
  - Easy for VMware:
    Suspend VM, then copy .vmem image file. ⇒ Done.
    Suitable only for “planned” tasks.
    Malware may potentially detect virtual machines.
  - kntdd by George Garner
    http://www.gmgsystemsinc.com/knttools/
  - F-Response
    http://www.f-response.com/
    Enables access to physical memory over iSCSI
  - MoonSols Windows Memory Toolkit by Mathieu Suiche:
    http://www.moonsols.com/products/
    win32dd (win64dd) Community (free) and Professional version
    Supports Microsoft Windows on 32bit and 64bit platform

Memory Forensics

- Software to acquire a memory image:
  - Plenty of tools available. Most for $$
  - Easy for VMware:
    Suspend VM, then copy .vmem image file. ⇒ Done.
    Suitable only for “planned” tasks.
    Malware may potentially detect virtual machines.
  - kntdd by George Garner
    http://www.gmgsystemsinc.com/knttools/
  - F-Response
    http://www.f-response.com/
    Enables access to physical memory over iSCSI
  - MoonSols Windows Memory Toolkit by Mathieu Suiche:
    http://www.moonsols.com/products/
    win32dd (win64dd) Community (free) and Professional version
    Supports Microsoft Windows on 32bit and 64bit platform

Memory Forensic

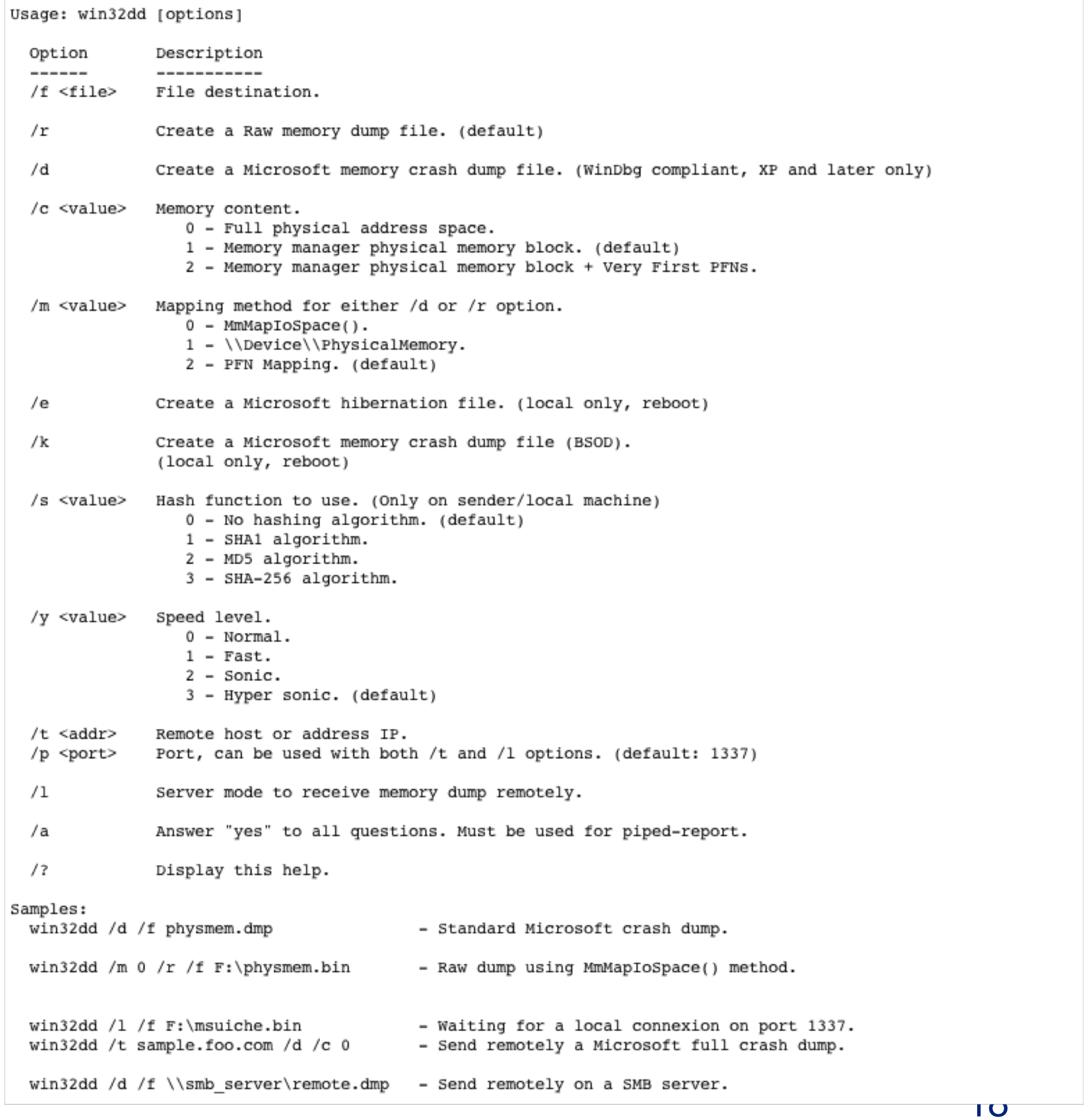
win32dd (win64dd) out of MoonSols Toolkit

The Swiss army knife for memory acquisition:

- Easy to use
- Produces images in either raw or **crashdump** formats
- Blurred and crisp memory images
- Three different methods to map memory
- Three hash functions: MD5, SHA-1, SHA-256
- Enables hibernate mode, forces crash (atomicity!)
- Can transfer memory image over network
- Works for XP, Vista and Win7 x86, x86_64

Memory Forensics

win32dd options:



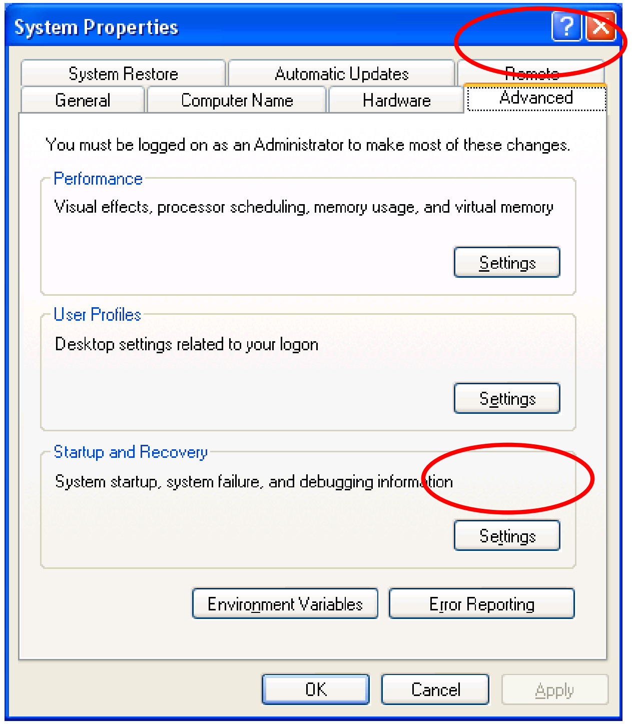
```
Usage: win32dd [options]

  Option       Description
  ------       -----------
  /f <file>    File destination.

  /r           Create a Raw memory dump file. (default)

  /d           Create a Microsoft memory crash dump file. (WinDbg compliant, XP and later only)

  /c <value>   Memory content.
                  0 - Full physical address space.
                  1 - Memory manager physical memory block. (default)
                  2 - Memory manager physical memory block + Very First PFNs.

  /m <value>   Mapping method for either /d or /r option.
                  0 - MmMapIoSpace().
                  1 - \\Device\\PhysicalMemory.
                  2 - PFN Mapping. (default)

  /e           Create a Microsoft hibernation file. (local only, reboot)

  /k           Create a Microsoft memory crash dump file (BSOD).
               (local only, reboot)

  /s <value>   Hash function to use. (Only on sender/local machine)
                  0 - No hashing algorithm. (default)
                  1 - SHA1 algorithm.
                  2 - MD5 algorithm.
                  3 - SHA-256 algorithm.

  /y <value>   Speed level.
                  0 - Normal.
                  1 - Fast.
                  2 - Sonic.
                  3 - Hyper sonic. (default)

  /t <addr>    Remote host or address IP.
  /p <port>    Port, can be used with both /t and /l options. (default: 1337)

  /l           Server mode to receive memory dump remotely.

  /a           Answer "yes" to all questions. Must be used for piped-report.

  /?           Display this help.

Samples:
  win32dd /d /f physmem.dmp               - Standard Microsoft crash dump.

  win32dd /m 0 /r /f F:\physmem.bin       - Raw dump using MmMapIoSpace() method.


  win32dd /l /f F:\msuiche.bin            - Waiting for a local connexion on port 1337.
  win32dd /t sample.foo.com /d /c 0       - Send remotely a Microsoft full crash dump.

  win32dd /d /f \\smb_server\remote.dmp   - Send remotely on a SMB server.
```

Memory Forensics

XP crash dump:

- Although win32dd supports crash dumps out of the box make sure you have full dumps enabled: (Default is minidumps only)

  Control Panel ⇒ System Properties



You must be logged on as an Administrator to make most of these changes.

Performance

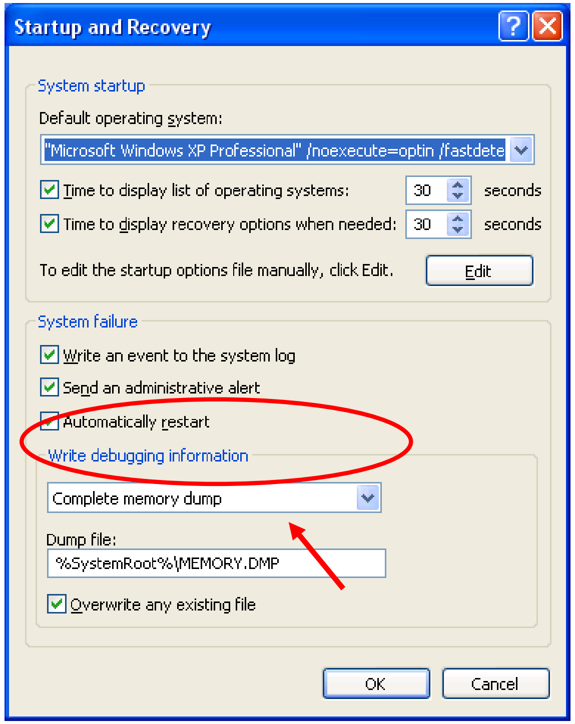
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information



System startup

Default operating system:

"Microsoft Windows XP Professional" /noexecute=optin /fastdete

☑ Time to display list of operating systems: 30 seconds

☑ Time to display recovery options when needed: 30 seconds

To edit the startup options file manually, click Edit.

System failure

☑ Write an event to the system log

☑ Send an administrative alert

☑ Automatically restart

Write debugging information

Complete memory dump

Dump file:

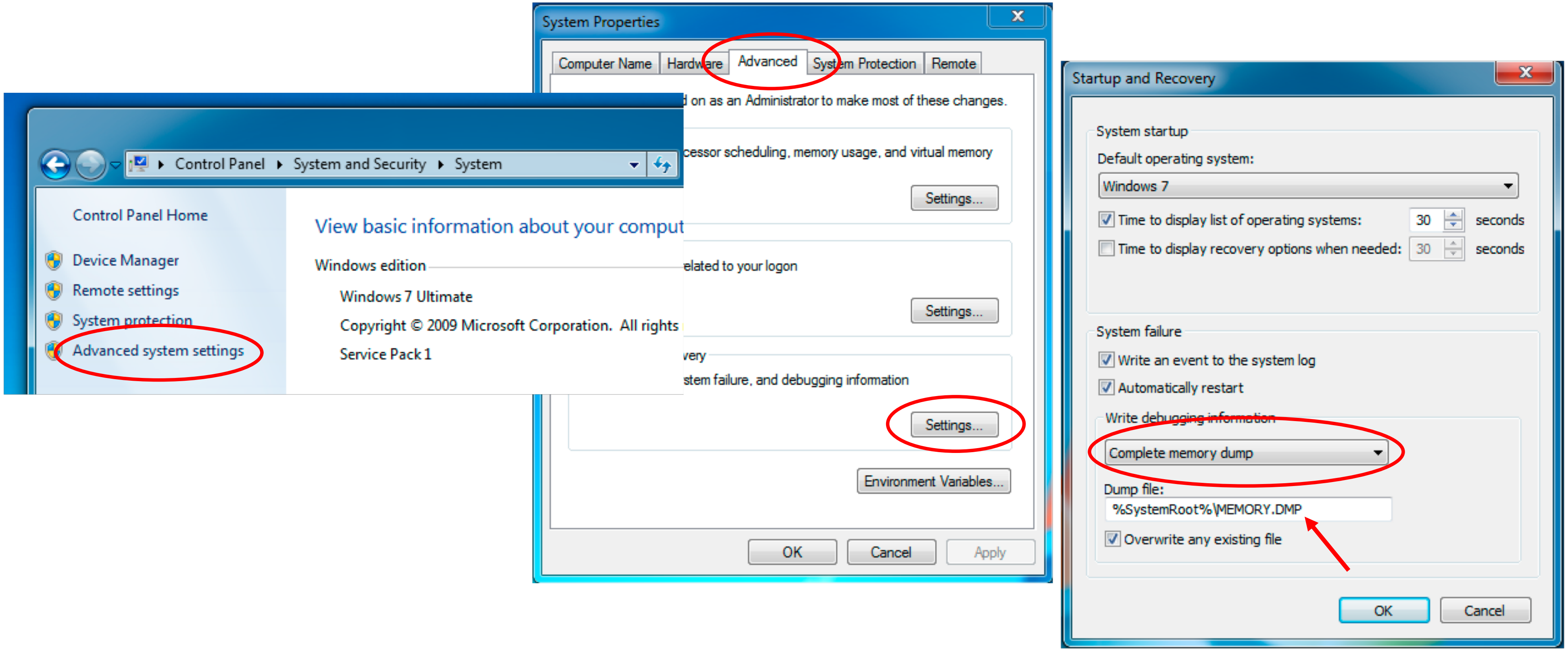
%SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

Win7 crash dump:

- Crashdumps

  Control Panel ⇒ System and Security ⇒ System



Control Panel ▸ System and Security ▸ System

Control Panel Home

Device Manager

Remote settings

System protection

Advanced system settings

View basic information about your comput

Windows edition

Windows 7 Ultimate

Copyright © 2009 Microsoft Corporation. All rights

Service Pack 1

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

d on as an Administrator to make most of these changes.

cessor scheduling, memory usage, and virtual memory

Settings...

elated to your logon

Settings...

very

stem failure, and debugging information

Settings...

Environment Variables...

OK Cancel Apply

Startup and Recovery

System startup

Default operating system: Windows 7

☑ Time to display list of operating systems: 30 seconds

□ Time to display recovery options when needed: 30 seconds

System failure

☑ Write an event to the system log

☑ Automatically restart

Write debugging information

Complete memory dump

Dump file: %SystemRoot%\MEMORY.DMP

☑ Overwrite any existing file

OK Cancel

Memory Forensics

Summary crash dumps:

- Crash dumps result in crisp images
- Depending on
  - Windows version: XP, Win7
  - Architecture: x86, x86_64
  - Memory 2GB > size > 2GB

  complete memory dumps may or may not be available.
- Mind to proper settings in the appropriate control panel section.
- See http://support.microsoft.com/kb/254649 for details.

Memory Forensics

Break

Memory Forensics

More Theory ...

Memory Forensics

- More on Windows crash dumps:

  Force a crash dump (blue screen) from the keyboard:

  http://msdn.microsoft.com/en-us/library/ff545499%28VS.85%29.aspx

  Enable crash Dumps in Registry:
- For PS2 Keyboards:

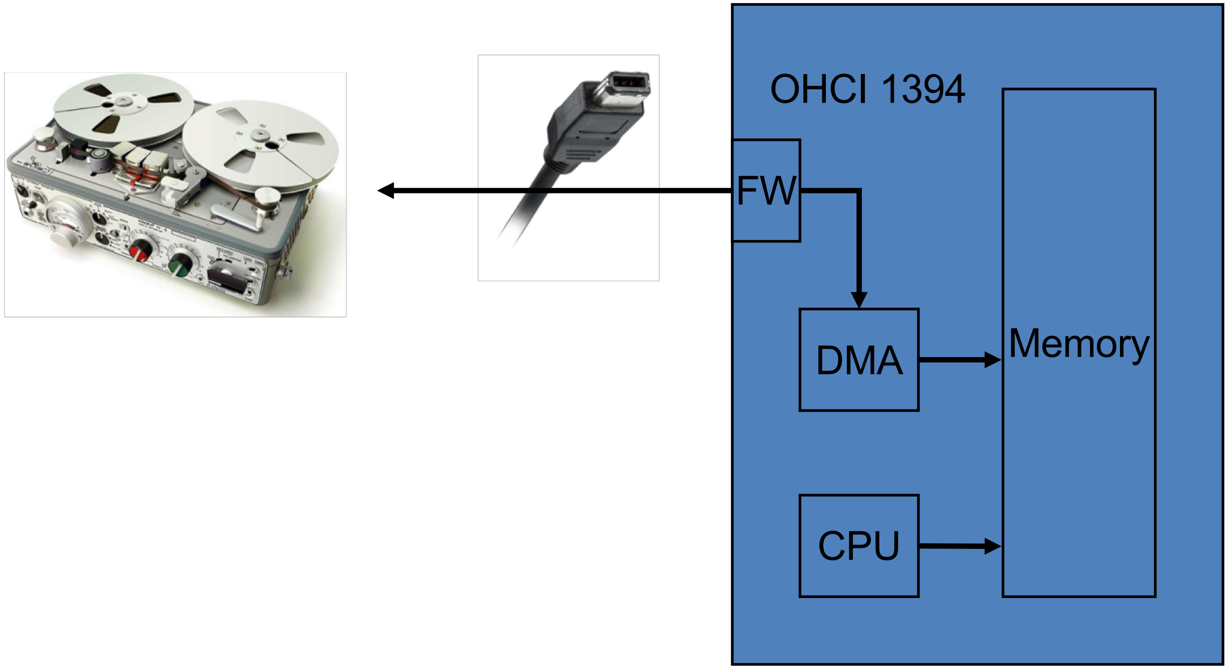
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\i8042prt\Parameters
  Create a named value:
  CrashOnCtrlScroll as REG_DWORD and set it to 0x01

- For USB keyboards:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\kbdhid\Parameters
  Create a named value:
  CrashOnCtrlScroll as REG_DWORD and set it to 0x01

- On keyboard: Right Control + twice “SCROLL lock” forces a crash and dumps memory to disk: Either as minidump (default) as full dump.

Memory Forensics

- Dump memory image over firewire:
  It’s a feature - not a bug!



Memory Forensics

Dump memory image over firewire and thunderbolt:

Advantage:

- No memory tampering

Disadvantage

- Only the first 4GB of memory are mapped.
- Special tools required.
  http://md.hudora.de/presentations/#firewire-pacsec
  http://www.storm.net.nz/projects/16
- http://www.breaknenter.org/projects/inception/
- http://www.breaknenter.org/2012/02/adventures-with-daisy-in-thunderbolt-dma-land-hacking-macs-through-the-thunderbolt-interface/
- .. and more firewire tools

Memory Forensics

Hands On Exercise

Memory Forensics

Use the tools presented to collect data from your system:

- Use WinAudit to get an overview of the system
- Collect process information
- Use Secunia Personal Software Inspector (PSI)
- Run some scanners
- Draw first conclusions from your findings

Memory Forensics

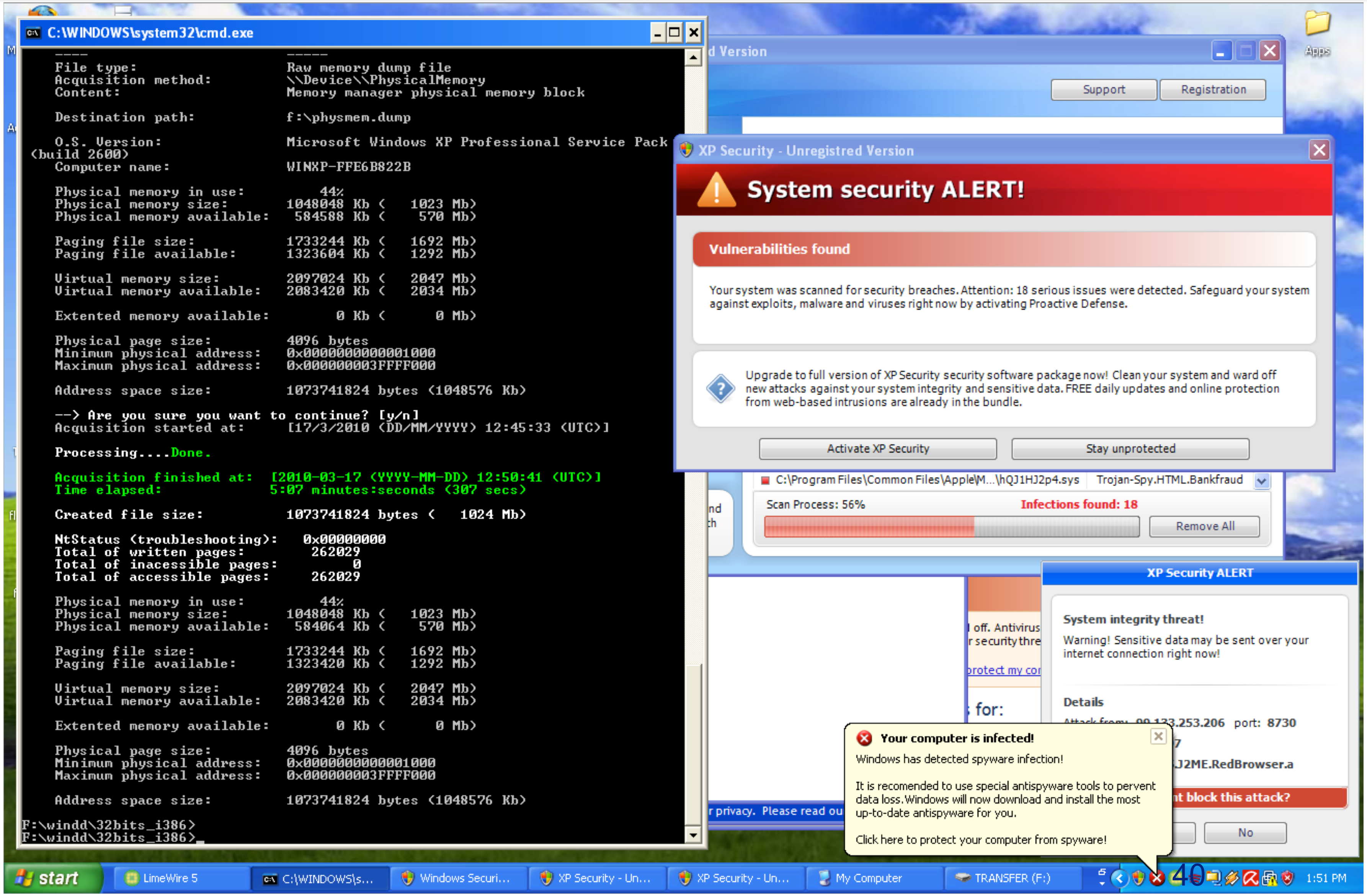
Analysing the memory image - bits and bytes:

- Oldie but Goldie: strings
- scalpel: A frugal, high performance file carver
  http://www.digitalforensicssolutions.com/Scalpel/
- chntpw: Registry analysis
  http://pogostick.net/~pnh/ntpasswd/
- volatility
  https://www.volatilesystems.com/default/volatility
- KnTTools by GMG Systems (commercial)
  http://gmgsystemsinc.com/fau/

Memory Forensics

Hands On Exercise

Memory Forensics



C:\WINDOWS\system32\cmd.exe

```
    ----                             -----
    File type:                       Raw memory dump file
    Acquisition method:              \\Device\\PhysicalMemory
    Content:                         Memory manager physical memory block

    Destination path:                f:\physmem.dump

    O.S. Version:                    Microsoft Windows XP Professional Service Pack
 (build 2600)
    Computer name:                   WINXP-FFE6B822B

    Physical memory in use:            44%
    Physical memory size:            1048048 Kb (   1023 Mb)
    Physical memory available:        584588 Kb (    570 Mb)

    Paging file size:                1733244 Kb (   1692 Mb)
    Paging file available:           1323604 Kb (   1292 Mb)

    Virtual memory size:             2097024 Kb (   2047 Mb)
    Virtual memory available:        2083420 Kb (   2034 Mb)

    Extented memory available:             0 Kb (      0 Mb)

    Physical page size:              4096 bytes
    Minimum physical address:        0x0000000000001000
    Maximum physical address:        0x000000003FFFF000

    Address space size:              1073741824 bytes (1048576 Kb)

    --> Are you sure you want to continue? [y/n]
    Acquisition started at:          [17/3/2010 (DD/MM/YYYY) 12:45:33 (UTC)]

    Processing....Done.

    Acquisition finished at:   [2010-03-17 (YYYY-MM-DD) 12:50:41 (UTC)]
    Time elapsed:              5:07 minutes:seconds (307 secs)

    Created file size:               1073741824 bytes (   1024 Mb)

    NtStatus (troubleshooting):        0x00000000
    Total of written pages:             262029
    Total of inacessible pages:              0
    Total of accessible pages:          262029

    Physical memory in use:            44%
    Physical memory size:            1048048 Kb (   1023 Mb)
    Physical memory available:        584064 Kb (    570 Mb)

    Paging file size:                1733244 Kb (   1692 Mb)
    Paging file available:           1323420 Kb (   1292 Mb)

    Virtual memory size:             2097024 Kb (   2047 Mb)
    Virtual memory available:        2083420 Kb (   2034 Mb)

    Extented memory available:             0 Kb (      0 Mb)

    Physical page size:              4096 bytes
    Minimum physical address:        0x0000000000001000
    Maximum physical address:        0x000000003FFFF000

    Address space size:              1073741824 bytes (1048576 Kb)

F:\windd\32bits_i386>
F:\windd\32bits_i386>_
```

XP Security - Unregistred Version

System security ALERT!

Vulnerabilities found

Your system was scanned for security breaches. Attention: 18 serious issues were detected. Safeguard your system against exploits, malware and viruses right now by activating Proactive Defense.

Upgrade to full version of XP Security security software package now! Clean your system and ward off new attacks against your system integrity and sensitive data. FREE daily updates and online protection from web-based intrusions are already in the bundle.

C:\Program Files\Common Files\Apple\M...\hQJ1HJ2p4.sys   Trojan-Spy.HTML.Bankfraud

Scan Process: 56%   Infections found: 18

XP Security ALERT

System integrity threat!

Warning! Sensitive data may be sent over your internet connection right now!

Details

Attack from: 90.133.253.206 port: 8730

J2ME.RedBrowser.a

nt block this attack?

Your computer is infected!

Windows has detected spyware infection!

It is recomended to use special antispyware tools to pervent data loss.Windows will now download and install the most up-to-date antispyware for you.

Click here to protect your computer from spyware!

Memory Forensics

Memory Forensics

- The System or VMware image provided, contains everything.
- Working with the tools:
  - strings/grep
  - scalpel
  - reged
  - Volatility
- Use the prepared memory image available at

  `Exercises/images/MEMORY-IMG2.DMP`

Memory Forensics

Situation:

You have a memory image taken from a laptop, which was suspected to be involved in a serious e-banking incident. It is to be assumed that some malware could be on it. You suspect it could be either Zeus or Gozi, as these two malware families are currently active in your country. You have two papers available describing these malware families.

Make yourself familiar with the malware families and what characteristics they have and how they can potentially be recognised.

It's now your job to find out what could have happened.

- *A memory image from the PC was drawn and is stored on the VMware image*
- *The registry was dumped too and is also available for investigation.*

Memory Forensics

First, we apply good old strings and grep to the memory image to extract ASCII data.

- Try to find answers for the following questions:
  - What information can be found?
  - Which applications were running?
  - Which URLs can be identified?
  - What was the user doing, just before drawing the image?
  - Are there indications for any malware?
  - What conclusions can be drawn?

- Commands, which may help:

```
$ cd Exercises
$ strings images/MEMORY-IMG2.DMP
$ grep ‘http:\/\/’ strings.txt > http.txt
$ grep ‘https:\/\/’ strings.txt > https.txt
$ grep ‘c:\\’ strings.txt > paths.txt
```

Memory Forensics

Memory Forensics

- Until now we have processed more or less easily recognisable data. We still have more questions:
  - Which processes were running?
  - Which network connections existed at that time?
  - Again: Is there any evidence for malware?
  - Again: What conclusions can be drawn?

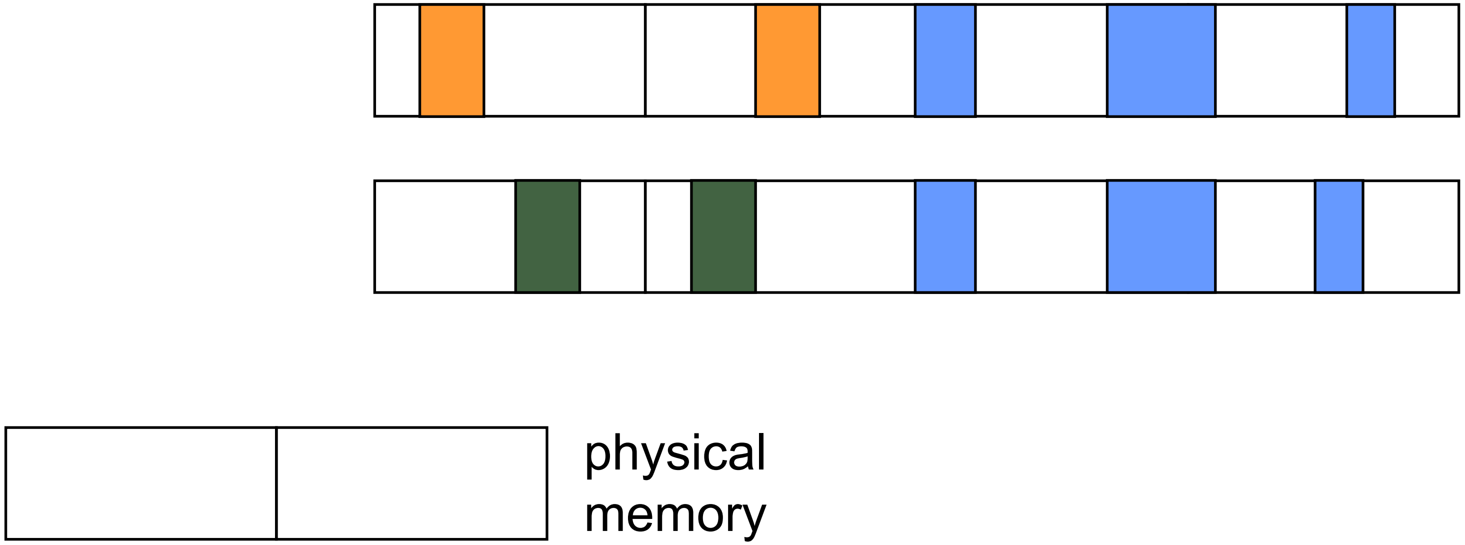
Memory Forensics

More Theory ...

Memory Forensics

Virtual / Physical memory

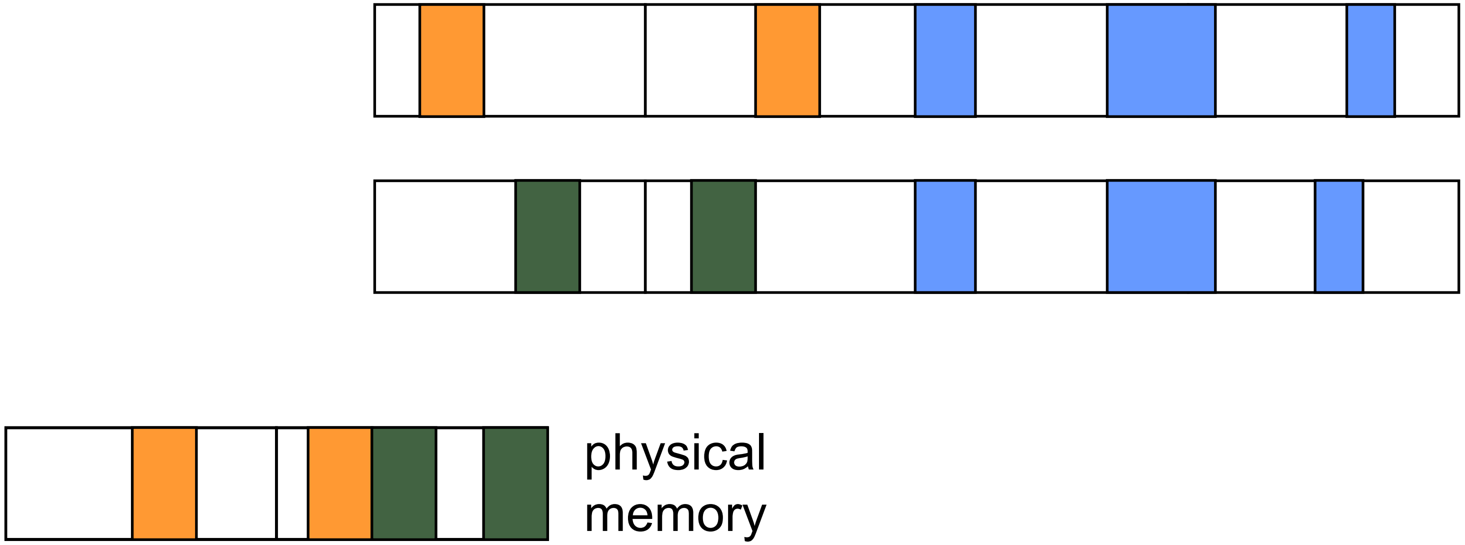
- Physical memory is divided into so-called “pages”.
- Allocated virtual memory is mapped onto physical memory page by page.



Memory Forensics

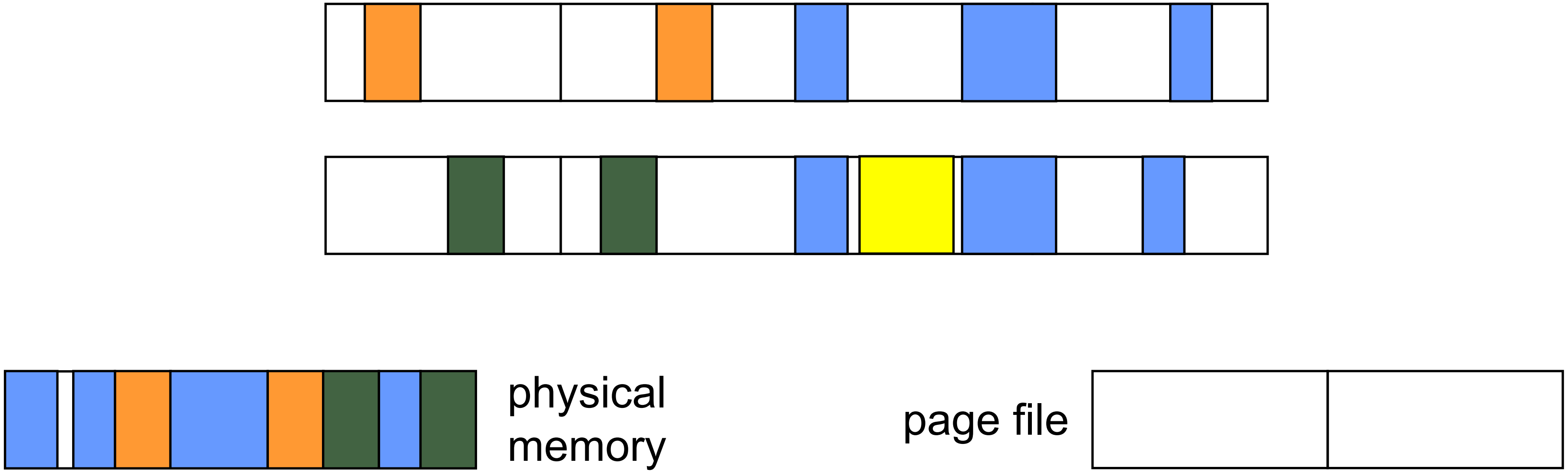
Virtual / Physical memory

The same page of physical memory can appear at different locations within the same address space or in different address spaces.



Virtual / Physical memory

Data can be moved from physical memory into a page file to clear some space.

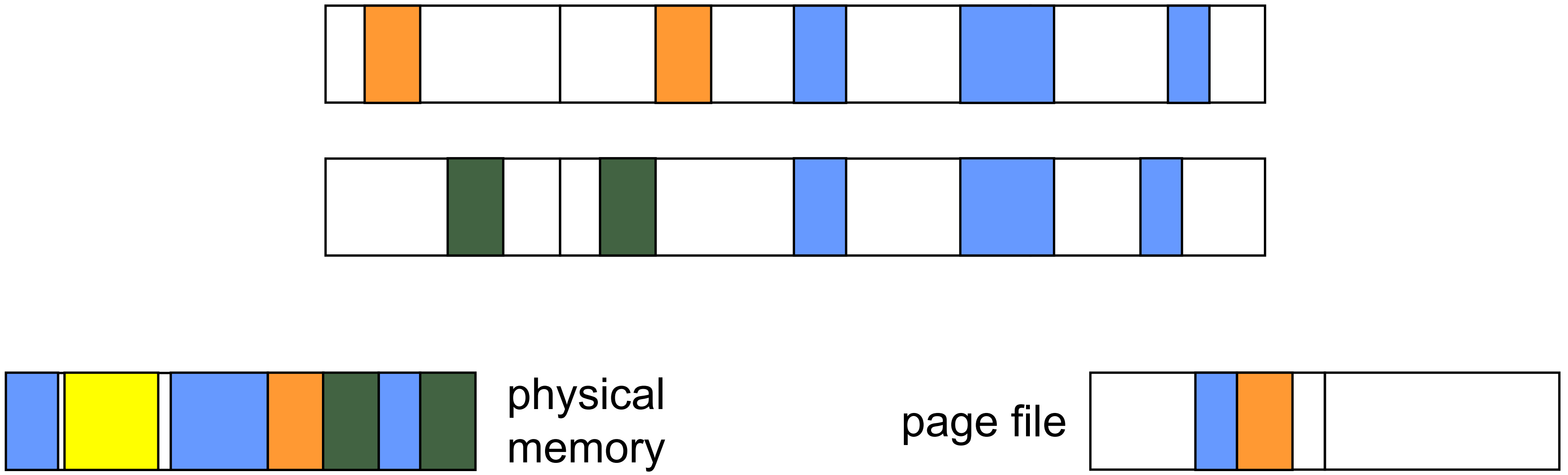


physical memory

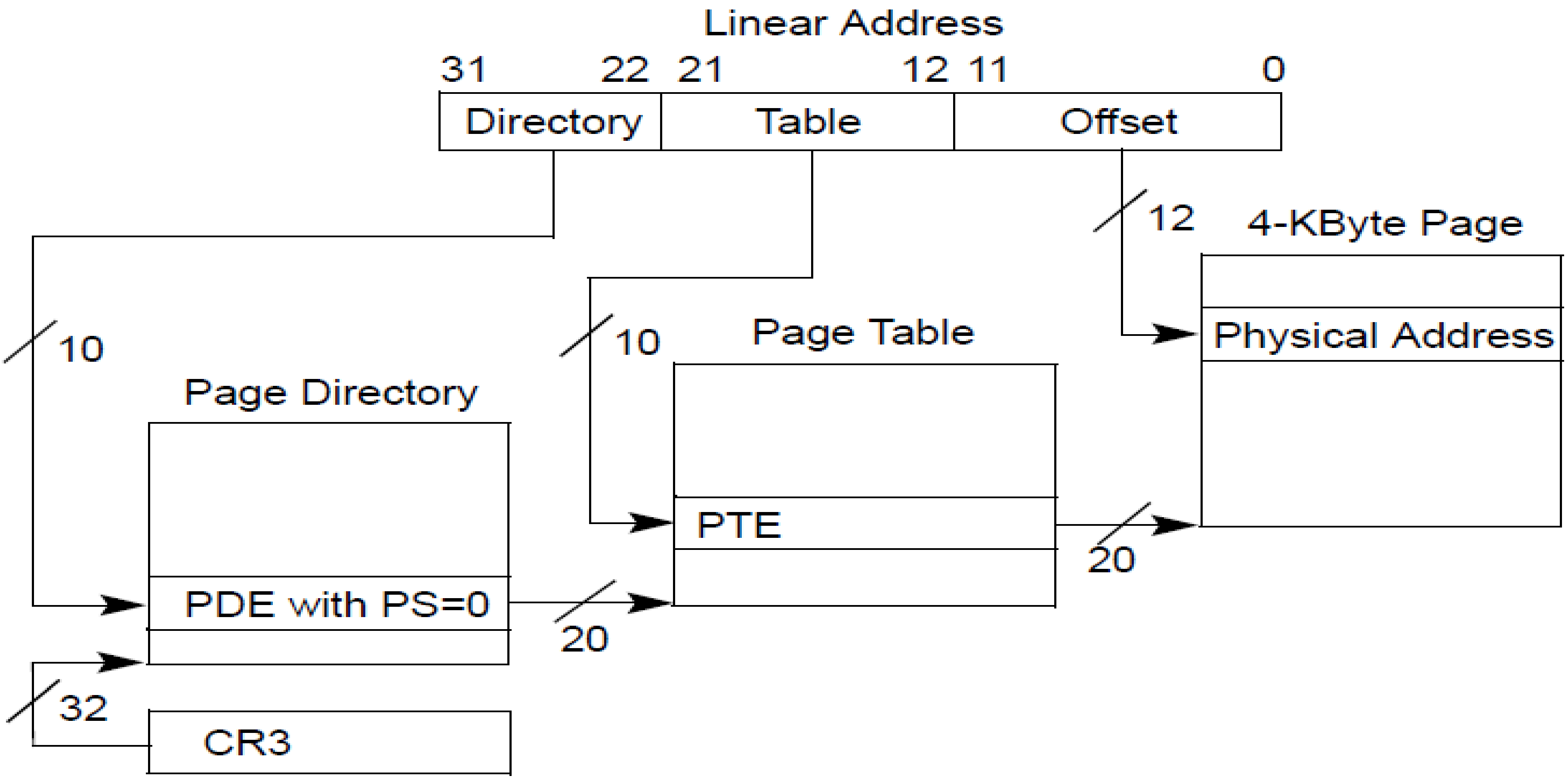
page file

Virtual / Physical memory

Data can be moved from physical memory into a page file to clear some space.



Memory Forensics



As an example: IA 32 address architecture.
(Intel Architecture Software Developer's Manual, Vol. 3A)
IA 64 is even more complex.

Memory Forensics

Volatility:

- Is the open source memory forensics framework for incident response and malware analysis.
- Is written in Python.
- Has many optional plugins
- Has a large community.
- Should run on any platform where Python is supported. Volatility has been tested on the following platforms:
  - Linux
  - Cygwin
  - Windows
  - OSX 10.5
- Supports Win XP, Vista, Win7

Memory Forensics

Volatility:

- The Volatility Framework currently provides the following extraction capabilities and more for memory samples:
  - Image date and time
  - Running processes
  - Open network sockets
  - Open network connections
  - DLLs loaded for each process
  - Open files for each process
  - Open registry handles for each process
  - A process' addressable memory
  - OS kernel modules
  - Mapping physical offsets to virtual addresses (strings to process)
  - Virtual Address Descriptor information
  - Scanning examples: processes, threads, sockets, connections,modules
  - Extract executables from memory samples
  - Transparently supports a variety of sample formats (ie, Crash dump, Hibernation, DD)
  - Automated conversion between formats

Memory Forensics

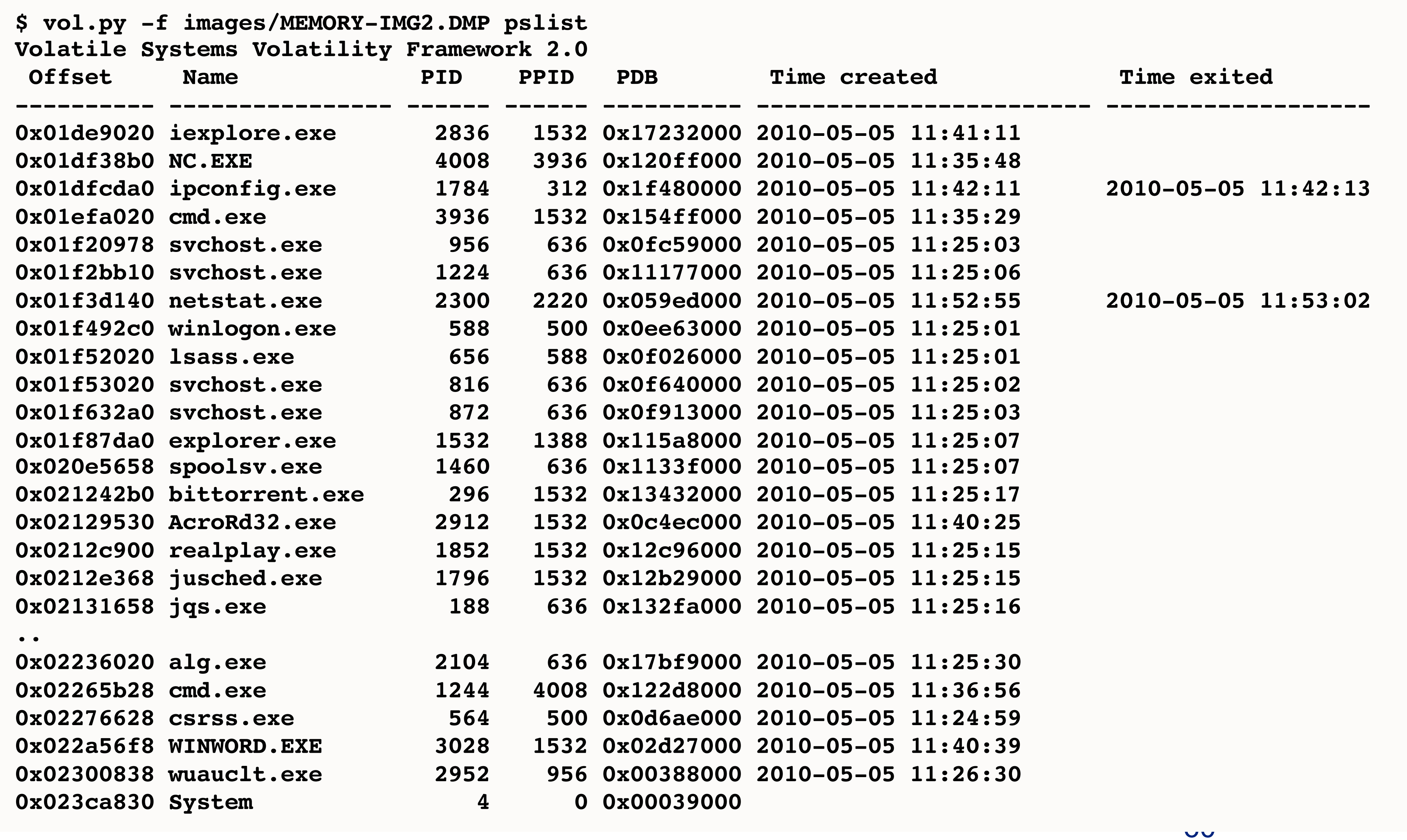
Hands On Exercise

Memory Forensics

Volatility:

```
$ vol.py -f images/MEMORY-IMG2.DMP imageinfo
Volatile Systems Volatility Framework 2.0
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP3x86, WinXPSP2x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : JKIA32PagedMemory (Kernel AS)
                     AS Layer2 : WindowsCrashDumpSpace32 (Exercises/images/MEMORY-IMG2.DMP)
                     AS Layer3 : FileAddressSpace (Exercises/images/MEMORY-IMG2.DMP)
                      PAE type : No PAE
                           DTB : 0x39000
                          KDBG : 0x8054cde0L
                          KPCR : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-05-05 11:54:02
     Image local date and time : 2010-05-05 11:54:02
          Number of Processors : 1
                    Image Type : Service Pack 3
```

Memory Forensics



```
$ vol.py -f images/MEMORY-IMG2.DMP pslist
Volatile Systems Volatility Framework 2.0
 Offset     Name              PID    PPID   PDB        Time created             Time exited
---------- ---------------- ------ ------ ---------- ------------------------ --------------------
0x01de9020 iexplore.exe       2836   1532 0x17232000 2010-05-05 11:41:11
0x01df38b0 NC.EXE             4008   3936 0x120ff000 2010-05-05 11:35:48
0x01dfcda0 ipconfig.exe       1784    312 0x1f480000 2010-05-05 11:42:11      2010-05-05 11:42:13
0x01efa020 cmd.exe            3936   1532 0x154ff000 2010-05-05 11:35:29
0x01f20978 svchost.exe         956    636 0x0fc59000 2010-05-05 11:25:03
0x01f2bb10 svchost.exe        1224    636 0x11177000 2010-05-05 11:25:06
0x01f3d140 netstat.exe        2300   2220 0x059ed000 2010-05-05 11:52:55      2010-05-05 11:53:02
0x01f492c0 winlogon.exe        588    500 0x0ee63000 2010-05-05 11:25:01
0x01f52020 lsass.exe           656    588 0x0f026000 2010-05-05 11:25:01
0x01f53020 svchost.exe         816    636 0x0f640000 2010-05-05 11:25:02
0x01f632a0 svchost.exe         872    636 0x0f913000 2010-05-05 11:25:03
0x01f87da0 explorer.exe       1532   1388 0x115a8000 2010-05-05 11:25:07
0x020e5658 spoolsv.exe        1460    636 0x1133f000 2010-05-05 11:25:07
0x021242b0 bittorrent.exe      296   1532 0x13432000 2010-05-05 11:25:17
0x02129530 AcroRd32.exe       2912   1532 0x0c4ec000 2010-05-05 11:40:25
0x0212c900 realplay.exe       1852   1532 0x12c96000 2010-05-05 11:25:15
0x0212e368 jusched.exe        1796   1532 0x12b29000 2010-05-05 11:25:15
0x02131658 jqs.exe             188    636 0x132fa000 2010-05-05 11:25:16
..
0x02236020 alg.exe            2104    636 0x17bf9000 2010-05-05 11:25:30
0x02265b28 cmd.exe            1244   4008 0x122d8000 2010-05-05 11:36:56
0x02276628 csrss.exe           564    500 0x0d6ae000 2010-05-05 11:24:59
0x022a56f8 WINWORD.EXE        3028   1532 0x02d27000 2010-05-05 11:40:39
0x02300838 wuauclt.exe        2952    956 0x00388000 2010-05-05 11:26:30
0x023ca830 System                4      0 0x00039000
```

Memory Forensics

Working with volatility:

- Use the different volatility commands in order to get interesting information out of the image:
  `pslist, psscan, connections, connscan, filescan etc.`
- Can you answer all remaining questions?

Memory Forensics

Searching for more information: Diving into the registry

The registry is a rich source of all sorts of information. Therefore it’s also a good place to search for hints.

reged is a powerful tool running on *NIXes to navigate within the Windows registry files. You can *search, change, add, delete* and even *dump* specific parts of the registry.

Memory Forensics

```
$ reged —e NTUSER.DAT
reged version 0.1 080526, (c) Petter N Hagen
Hive <NTUSER.DAT> name (from header): < Settings\Peter Haag\ntuser.dat>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x10b000 is not 'hbin', assuming file contains garbage at end
File size 1310720 [140000] bytes, containing 143 pages (+ 1 headerpage)
Used for data: 11873/1049416 blocks/bytes, unused: 479/35544 blocks/bytes.

Simple registry editor. ? for help.

> ?
Simple registry editor:
hive [<n>]              - list loaded hives or switch to hive numer n
cd <key>                - change current key
ls | dir [<key>]        - show subkeys & values,
cat | type <value>      - show key value
dump <value> [<file>]   - dump key value to file. default file: <value>
hex <value>             - hexdump of value data
ck [<keyname>]          - Show keys class data, if it has any
nk <keyname>            - add key
dk <keyname>            - delete key (must be empty)
ed <value>              - Edit value
nv <type#> <valuename> - Add value
dv <valuename>          - Delete value
delallv                 - Delete all values in current key
rdel <keyname>          - Recursively delete key & subkeys
ek <filename> <prefix> <keyname>  - export key to <filename> (Windows .reg file format)
debug                   - enter buffer hexeditor
st [<hexaddr>]          - debug function: show struct info
q                       - quit
```

Memory Forensics

Regedt

- Make yourself familiar with reged
- Based on the finding and conclusions, search for maybe relevant keys in this case.
  - Search for suspected keys.
  - Can you confirm what you suspected?

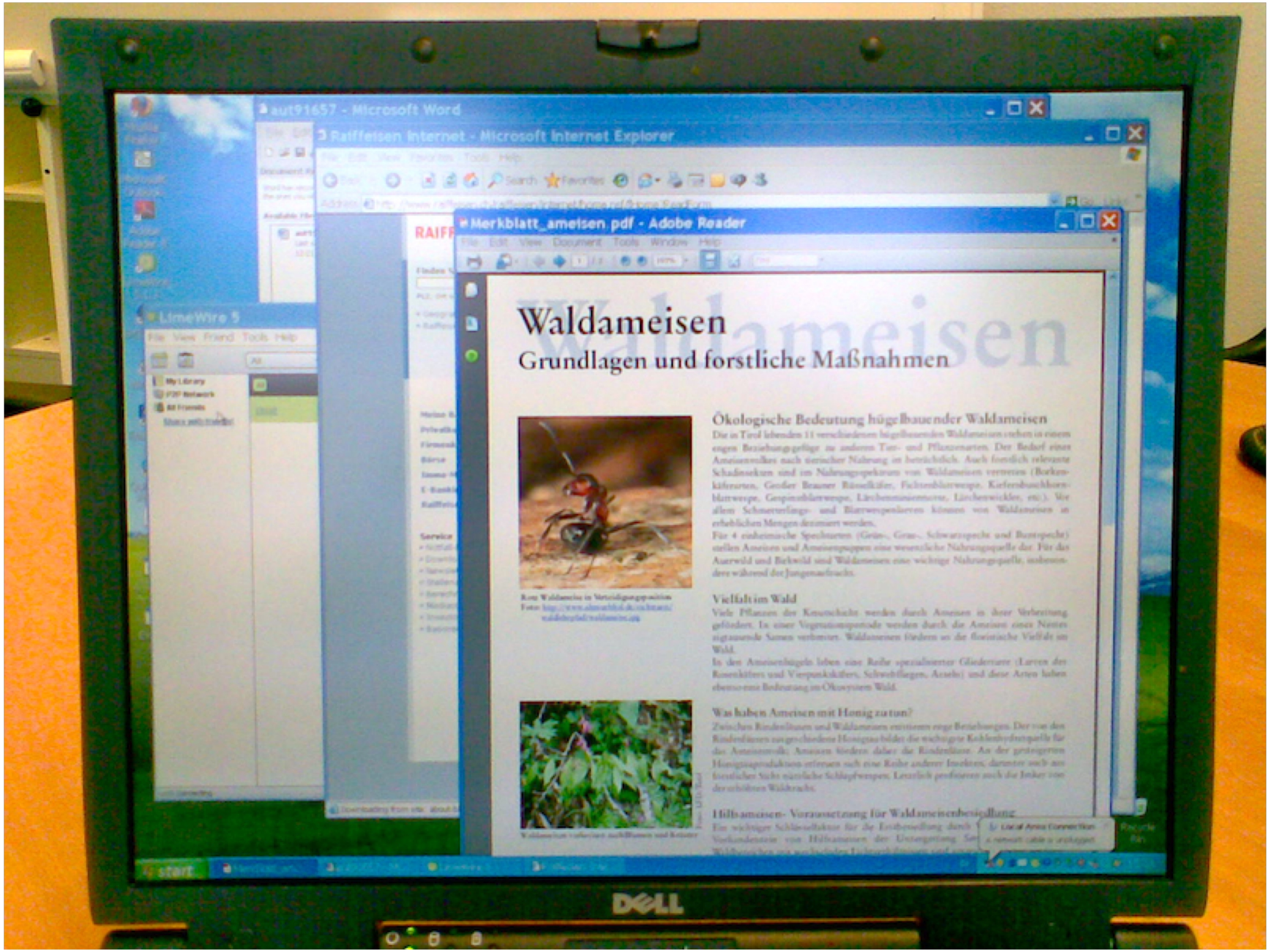
Memory Forensics

And finally ...

Memory Forensics

- The glory details:
- Adobe Reader 8.0
  - Document: Waldameisen: Grundlagen und forstliche Massnahmen.
- MS Word:
  - Document: Bekämpfung von Obstbauschädlingen.
- Internet Explorer
  - URL: www.tagesanzeiger.ch
  - URL: www.raiffeisen.ch (eBanking)
  - URL: www.gmail.com
    Account piotr.oscarovitch@gmail.com
    Password Ru$$1@RU
- Limewire, searching for Photoshop
- Infected with Gozi
- Remote controlled: hidden netcat with cmd.exe attached.

Memory Forensics


aut91657 - Microsoft Word
Raiffeisen Internet - Microsoft Internet Explorer
Merkblatt_ameisen.pdf - Adobe Reader
LimeWire 5
Waldameisen
Grundlagen und forstliche Maßnahmen
Ökologische Bedeutung hügelbauender Waldameisen
Vielfalt im Wald
Was haben Ameisen mit Honig zu tun?
Hilfsameisen- Voraussetzung für Waldameisenbesiedlung
start
DELL

Memory Forensics

Memory Forensics

Links

- Process Explorer, Autorun
  http://technet.microsoft.com/en-us/sysinternals/default.aspx
- WinAudit
  http://www.pxserver.com/WinAudit.htm
- F-Secure Blacklight
  http://www.f-secure.com/en_EMEA/security/tools/blacklight/
- GMER
  http://www.gmer.net/
- Secunia PSI
  http://secunia.com/vulnerability_scanning/online/?task=intro
- Andreas Schusters Forensics Blog
  http://computer.forensikblog.de/en/
  Many thanks to my colleague Andreas for using part of his materials!!