SWINBURNE UNIVERSITY OF TECHNOLOGY

ICT30010 eForensic Fundamentals

Lecture 3

Computer Forensics

Troy Pretty

Digital Forensic Analyst

Outline and learning goals

- Analysis Types
  - Static Analysis
  - Live Analysis
- File analysis
  - Windows registry / event log analysis
  - User files
- Collecting volatile data in Windows
  - Windows memory analysis

Static Analysis

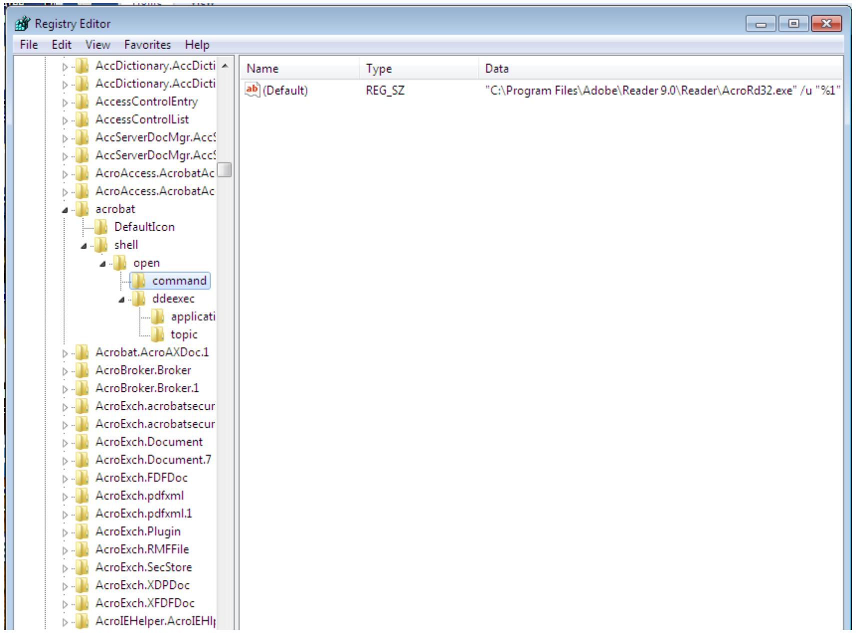
- Static analysis
  - Sometimes 'dead box analysis', 'non-volatile analysis'
  - Observation of static offline storage of a machine
- Static data analysis includes items stored in
  - ROM
  - Hard disk drives and their contents
  - USB devices
- Specific items that may be of interest are
  - BIOS settings
  - Registry settings
  - Event logs
  - User files

BIOS settings

- Date
- Time
- Boot sequence
- Hardware configuration

Registry settings

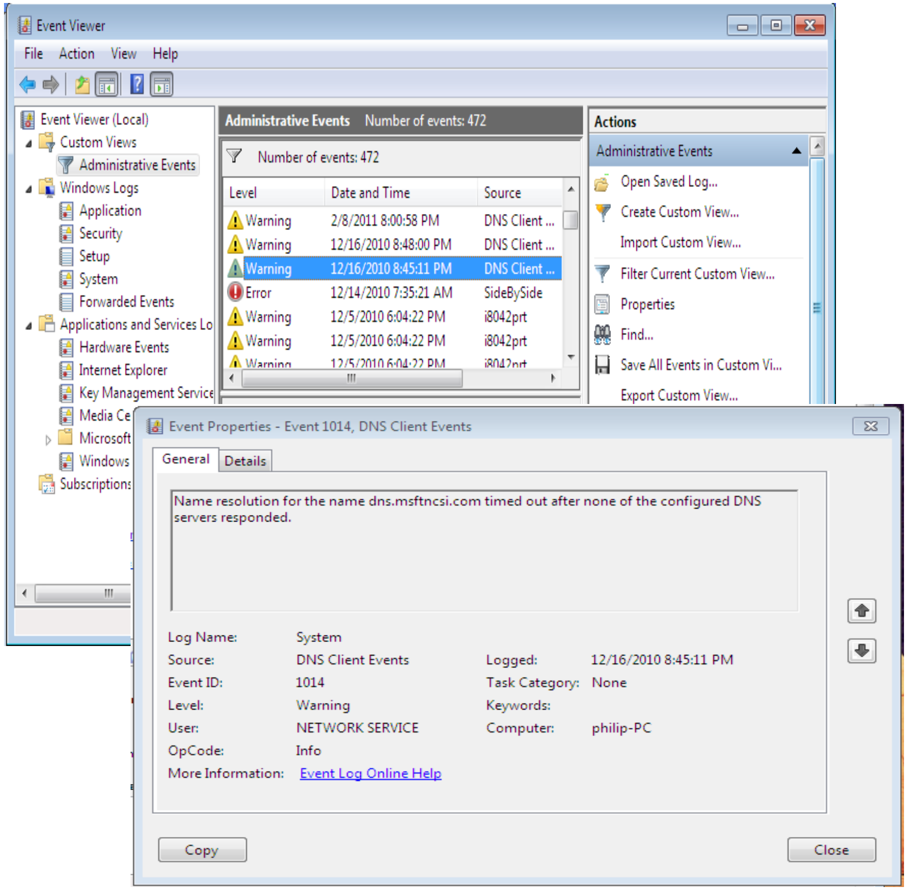
- The registry in Windows is a database of configuration information
- Structured as keys and values
- Some parts of the registry are volatile
- Some entries in the registry will have time stamps
- Registry analysis is often useful in investigations
  - Registry can be accessed using the regedit.exe command from the CLI



Name	Type	Data
(Default)	REG_SZ	"C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe" /u "%1"

Event Logs

- Significant (and not so significant) events are recorded in Windows event logs
- Windows records events about
  - Applications
  - Security
  - System events
  - Expanding in new versions
- Event log viewer



Administrative Events Number of events: 472

Number of events: 472

Level	Date and Time	Source
Warning	2/8/2011 8:00:58 PM	DNS Client ...
Warning	12/16/2010 8:48:00 PM	DNS Client ...
Warning	12/16/2010 8:45:11 PM	DNS Client ...
Error	12/14/2010 7:35:21 AM	SideBySide
Warning	12/5/2010 6:04:22 PM	i8042prt
Warning	12/5/2010 6:04:22 PM	i8042prt
Warning	12/5/2010 6:04:22 PM	i8042prt

Name resolution for the name dns.msftncsi.com timed out after none of the configured DNS servers responded.

Log Name:	System		
Source:	DNS Client Events	Logged:	12/16/2010 8:45:11 PM
Event ID:	1014	Task Category:	None
Level:	Warning	Keywords:	
User:	NETWORK SERVICE	Computer:	philip-PC
OpCode:	Info		
More Information:	Event Log Online Help		

User Files

- Many different types of files
  - .doc(x), .pdf, .xls(x) etc
- Saved in user accessible locations
- Often user files contain metadata
  - Data about the file
  - May include revision number, author of that revision, when last printed, GPS.
  - Useful during an investigation

Locating User Files

- Allocated Files
  - Entry exists in file allocation table
  - File is on the disk
  - File can be viewed
- Deleted Files
  - File entry marked for deletion (still exists)
  - File is on the disk
  - Hidden in windows, can be viewed with a forensic tool

Locating User Files

- Unallocated file
  - File entry does not exist
  - File now in unallocated space
  - Locate sectors of the file and manually recover
- Renamed Files
  - File extension changed
  - ie. secret.doc renamed secret.jpg
  - Signature Analysis
    - Review file header (first few bytes of file)
    - Look for mismatches

Live Analysis

- Live analysis
  - Observation of an active machine
  - Includes RAM and items resident within RAM such as running processes, open ports
  - Can capture RAM and reconstruct on a different machine
    - Particularly easy in a virtual environment such as VMWare
    - 3rd Party Tools – Will overwrite RAM
- Live analysis is of an active machine
  - Want to observe or collect data that can be lost when the machine is powered down
  - Live analysis needs great care
    - By observing the system the analyst inevitably changes it
    - All actions must be documented and recorded

Live Analysis

- Locard's principle: Locard's exchange principle states that "with contact between two items, there will be an exchange"
  - Locard's principle is fundamental to forensics
  - But it also applies to investigation – by investigating the system we change it

Live Analysis

- Live analysis items of interest:
  - System time
  - OS Details/Version
  - Logged on users
  - Open files
  - Active processes
  - Port mappings
  - Process memory
  - Network status
  - Clipboard contents
  - Active processes
  - Mapped drives

- Worth noting that most active systems will change without analyst's intervention
  - External user log in and remove incriminating data
  - Windows can generate a 'restore point' every 24 hours
  - Windows can carry out limited defragmentation every 36 hours

Live analysis methodology

- Local response
  - Sitting at the machine, entering commands at the keyboard and saving results to a removable device or network device that appears as a local device
  - Advantage is that it is quick
  - Disadvantage is that not scalable when many machines involved and much more likely to affect evidence being collected
- Remote response
  - Accessing the machine via a network
  - Advantage is that it is scalable where many machines involved
  - Disadvantage is that it can be slow or difficult to set up network connections
- Hybrid approach is a mixture of both

Guidelines for a live analysis (1)

- Adhere to the site's security policy which should include Incident Handling response procedure
- Capture an accurate picture of the system as soon as possible
- Keep detailed notes including dates and times. You may be called upon to give evidence months or even years later
- Specify whether using UTC, local time or system clock time in notes
- Minimise changes to system as you collect data from it
- (From IETF RFC 3227)

Guidelines for a live analysis (2)

- Isolate the system from the possibility of external change
- If faced with the choice, collect data first, do the analysis later
- Make sure you have well-defined, tested procedures for incident response. Use automation where possible
- For each device on the computer use a methodical approach that follows the guidelines laid down in the collection procedure
- Proceed from volatile to less volatile data
- Make a bit level copy of system's media

Guidelines for a live analysis (3)

- Do not shutdown the system until evidence collection completed
- Minimise use of programs that change access time of all files on the system
- Be careful about removing external access. It may trigger switches that remove evidence
- Respect privacy rules.

Guidelines for a live analysis (4)

- Make sure you have proper authorisation for the analysis
- Make sure you observe legal requirements regarding evidence
- Document each step
- Where feasible use checksums to ensure data has not been tampered with
- Record system times, in particular noting any clock drift
- Make note of people present, their reactions, what they observed

Live analysis of a windows machine

- Order of volatility important to consider
  - Long lived processes
    - daemons in unix, services in Windows
  - Short-lived processes
    - carry out some specific action (perhaps in response to a command) and then exit from RAM
  - TCP connections will timeout within seconds

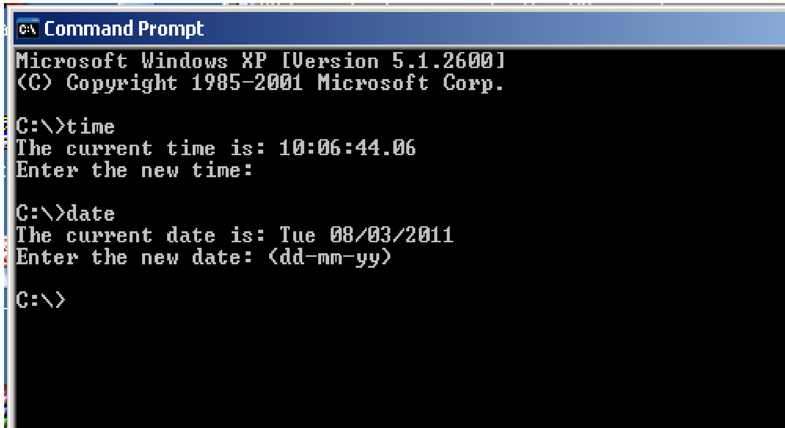
- RFC3227 has the following example of order of volatility
  - Registers, cache
  - Routing table, arp cache, process table, system statistics
  - Temporary file systems
  - Disk
  - Remote logging data
  - Physical configuration
  - Archival media

Live analysis toolkit

- Rather than using software loaded from the machine under investigation, a trusted set of evidence collection programs should be used
  - Should be on a read-only medium such as a CD
  - Should be statically linked and not require any libraries from the machine under investigation
- Should include programs to do the following
  - Examining processes
  - Examining system state
  - Generating checksums
  - Capturing memory dumps

System time

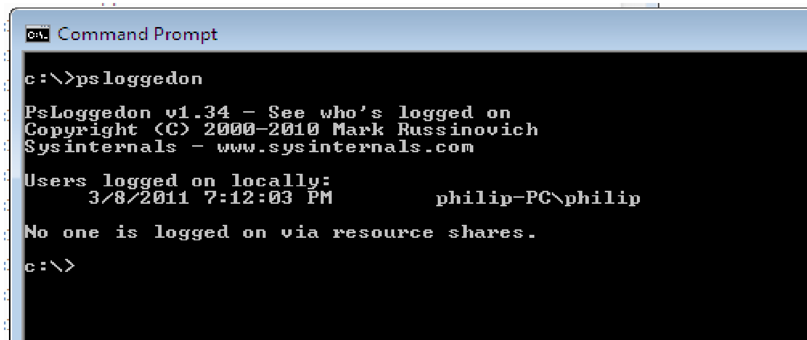
- Should check system time
  - May need to correlate with other events
  - Replay attacks may require a specific time
- System time can be obtained in Windows from mscmd window
  - `time`, `date` or `date/t`



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>time
The current time is: 10:06:44.06
Enter the new time:

C:\>date
The current date is: Tue 08/03/2011
Enter the new date: (dd-mm-yy)

C:\>
```

Logged on users

- What users are logged onto this machine?
- May be logged on remotely
  - `Net sessions`
    - Native to Windows
  - `PsLoggedOn.exe`
  - `LogonSessions.exe`
    - Available from technet.microsoft.com



```
c:\>psloggedon

PsLoggedon v1.34 - See who's logged on
Copyright (C) 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     3/8/2011 7:12:03 PM          philip-PC\philip

No one is logged on via resource shares.

c:\>
```

Open Files

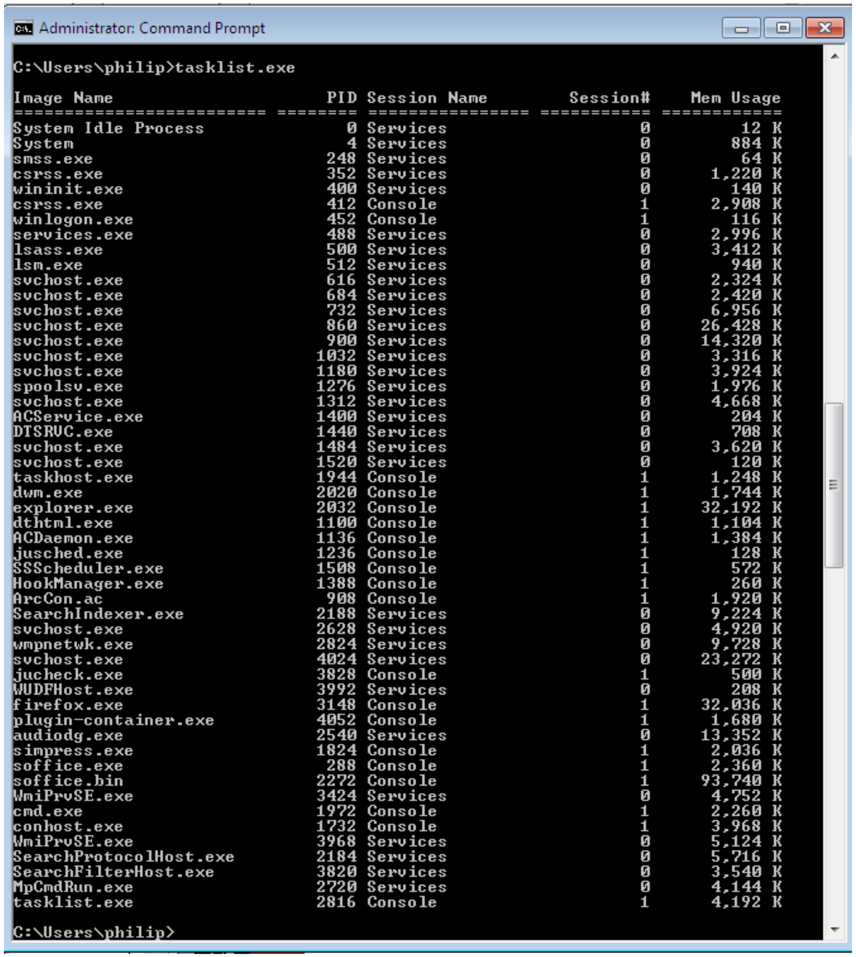
- `Net file, psfile` and `openfiles`
  - Will all show files opened remotely
  - Openfiles will show locally opened files

Active processes

- Important to know what processes active
  - Task manager simplest, but usually want more information than it provides
- Information needed includes
  - Full path to the executable image
  - Command line used to launch process (if any)
  - Time process has been running
  - Security and user context in which process running
  - Modules (DLLs) loaded by process
  - Memory contents of the process

Active processes

- Tasklist.exe
  - Native to Windows
- Pslist
  - Additional information such as memory usage
- ListDLLs
  - Information about dynamically linked libraries



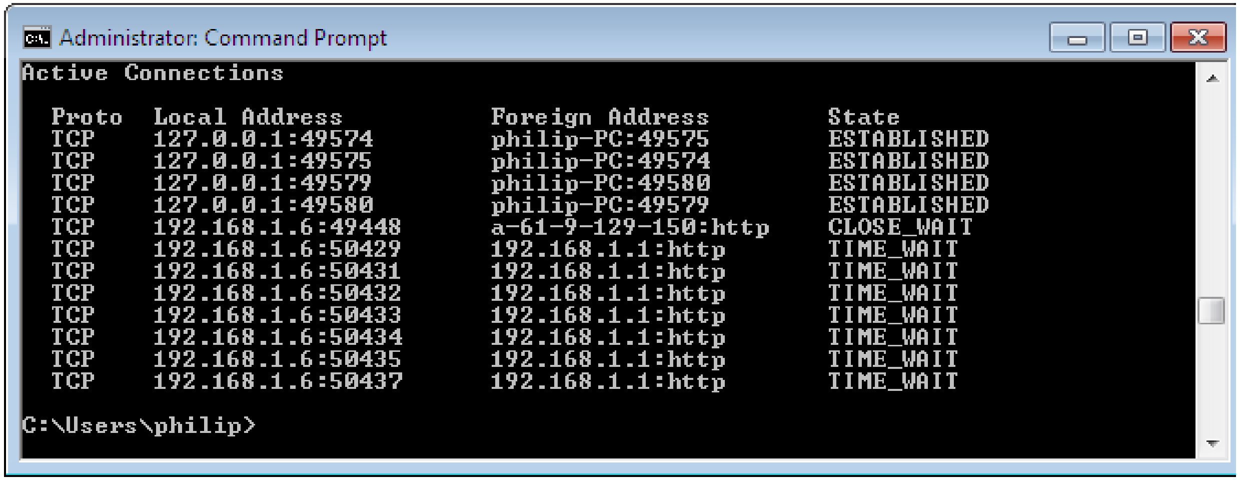
```
C:\Users\philip>tasklist.exe

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         12 K
System                           4 Services                   0        884 K
smss.exe                       248 Services                   0         64 K
csrss.exe                      352 Services                   0      1,220 K
wininit.exe                    400 Services                   0        140 K
csrss.exe                      412 Console                    1      2,908 K
winlogon.exe                   452 Console                    1        116 K
services.exe                   488 Services                   0      2,996 K
lsass.exe                      500 Services                   0      3,412 K
lsm.exe                        512 Services                   0        940 K
svchost.exe                    616 Services                   0      2,324 K
svchost.exe                    684 Services                   0      2,420 K
svchost.exe                    732 Services                   0      6,956 K
svchost.exe                    860 Services                   0     26,428 K
svchost.exe                    900 Services                   0     14,320 K
svchost.exe                   1032 Services                   0      3,316 K
svchost.exe                   1180 Services                   0      3,924 K
spoolsv.exe                   1276 Services                   0      1,976 K
svchost.exe                   1312 Services                   0      4,668 K
ACService.exe                 1400 Services                   0        204 K
DTSRVC.exe                    1440 Services                   0        708 K
svchost.exe                   1484 Services                   0      3,620 K
svchost.exe                   1520 Services                   0        120 K
taskhost.exe                  1944 Console                    1      1,248 K
dwm.exe                       2020 Console                    1      1,744 K
explorer.exe                  2032 Console                    1     32,192 K
dthtml.exe                    1100 Console                    1      1,104 K
ACDaemon.exe                  1136 Console                    1      1,384 K
jusched.exe                   1236 Console                    1        128 K
SSScheduler.exe               1508 Console                    1        572 K
HookManager.exe               1388 Console                    1        260 K
ArcCon.ac                      908 Console                    1      1,920 K
SearchIndexer.exe             2188 Services                   0      9,224 K
svchost.exe                   2628 Services                   0      4,920 K
wmpnetwk.exe                  2824 Services                   0      9,728 K
svchost.exe                   4024 Services                   0     23,272 K
jucheck.exe                   3828 Console                    1        500 K
WUDFHost.exe                  3992 Services                   0        208 K
firefox.exe                   3148 Console                    1     32,036 K
plugin-container.exe          4052 Console                    1      1,680 K
audiodg.exe                   2540 Services                   0     13,352 K
simpress.exe                  1824 Console                    1      2,036 K
soffice.exe                    288 Console                    1      2,360 K
soffice.bin                   2272 Console                    1     93,740 K
WmiPrvSE.exe                  3424 Services                   0      4,752 K
cmd.exe                       1972 Console                    1      2,260 K
conhost.exe                   1732 Console                    1      3,968 K
WmiPrvSE.exe                  3968 Services                   0      5,124 K
SearchProtocolHost.exe        2184 Services                   0      5,716 K
SearchFilterHost.exe          3820 Services                   0      3,540 K
MpCmdRun.exe                  2720 Services                   0      4,144 K
tasklist.exe                  2816 Console                    1      4,192 K

C:\Users\philip>
```

Port mappings

- A host may be running a server
  - Webserver, telnet server, email server
- A server listens for messages on a particular port number
  - Eg http traffic is usually directed to port 80
- Important to know what processes are listening to which ports
  - Can be done with netstat, fport, tcpvcon
- Externally, can be done via a port scan using tools such as nmap
  - Needs to be done with caution – Consider corporate policy

Network Status

- Netstat
  - Shows connections and their states
- Ipconfig
  - Shows network interface cards and IP addresses



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49574        philip-PC:49575        ESTABLISHED
  TCP    127.0.0.1:49575        philip-PC:49574        ESTABLISHED
  TCP    127.0.0.1:49579        philip-PC:49580        ESTABLISHED
  TCP    127.0.0.1:49580        philip-PC:49579        ESTABLISHED
  TCP    192.168.1.6:49448      a-61-9-129-150:http    CLOSE_WAIT
  TCP    192.168.1.6:50429      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50431      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50432      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50433      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50434      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50435      192.168.1.1:http       TIME_WAIT
  TCP    192.168.1.6:50437      192.168.1.1:http       TIME_WAIT

C:\Users\philip>
```

Clipboard contents and command history

- Can be useful to see what information has been cut or copied
  - Contents is stored in clipboard
  - Can be obtained by opening `notepad.exe` and `Control + V` to paste contents
- Command history can be obtained from
  - `Windows: Doskey /history`
  - `Linux: .bash_history file`

Mapped drives and shares

- What are the drive mappings?
  - Drive mappings may have been created maliciously
  - May be relevant in IP theft investigations
- `di.exe`
  - Shows mapping, type, file system and space
- `net use`
  - Built in windows command (shows mapping only)
- Shares are areas of the computer's hard disk that is available for others on the network to use
  - More difficult to identify
  - CLI command `share.exe`

Memory capture and analysis

- Capture and analyse the contents of RAM
- Many tools available to capture memory
  - Nigilant32, ProDiscover, KnTDD, MDD, Win32dd, FTK Imager, Magnet RAM to name a few
  - If virtualization (such as VMWare) being used then if the session has been suspended then the contents of memory will have been written to a .vmem file
  - Hibernation also writes memory to a file

Memory analysis

- A number of commercial systems allow memory, once captured, to be analysed (parsed)
  - HBGary Responder
  - Memoryze
- Open Source Analysis
  - Volitility Framework
- Can determine information such as
  - Active processes
  - Open files
  - Loaded modules

Live analysis in a virtual environment

- An environment such as vmware can be particularly useful for live analysis
- The virtualisation software writes a snapshot file that enables the environment to be reconstructed at a later time
- If an investigation is of a virtual environment it may be that such a file can be used in an analysis

Live analysis summary

- Main goal is to capture volatile information
  - Needs great care – by observing the system, you change it
    - Locard's principle
- Can be done locally, remotely or both
- Volatile information will be gone when the system shuts down, or may timeout or otherwise change without intervention
- In this unit you are not expected to know all these commands, but to appreciate that there are a large number of options for live analysis

Summary

- Computer forensics involves the capture and analysis of volatile and non-volatile data
- The analysis of volatile data needs to be carried out with caution
    - Live analysis will modify the system being investigated
    - Many tools available
- Analysis of non-volatile data more robust
    - Includes BIOS, Registry, Event logs, Device information and User files

References

- References:
  - H. Carvey, “Windows Forensic Analysis”, 2009
  - IETF RFC3227 “Guidelines for Evidence Collection and Archiving”, 2002
  - B. Carrier, “File System Forensic Analysis”, 2005