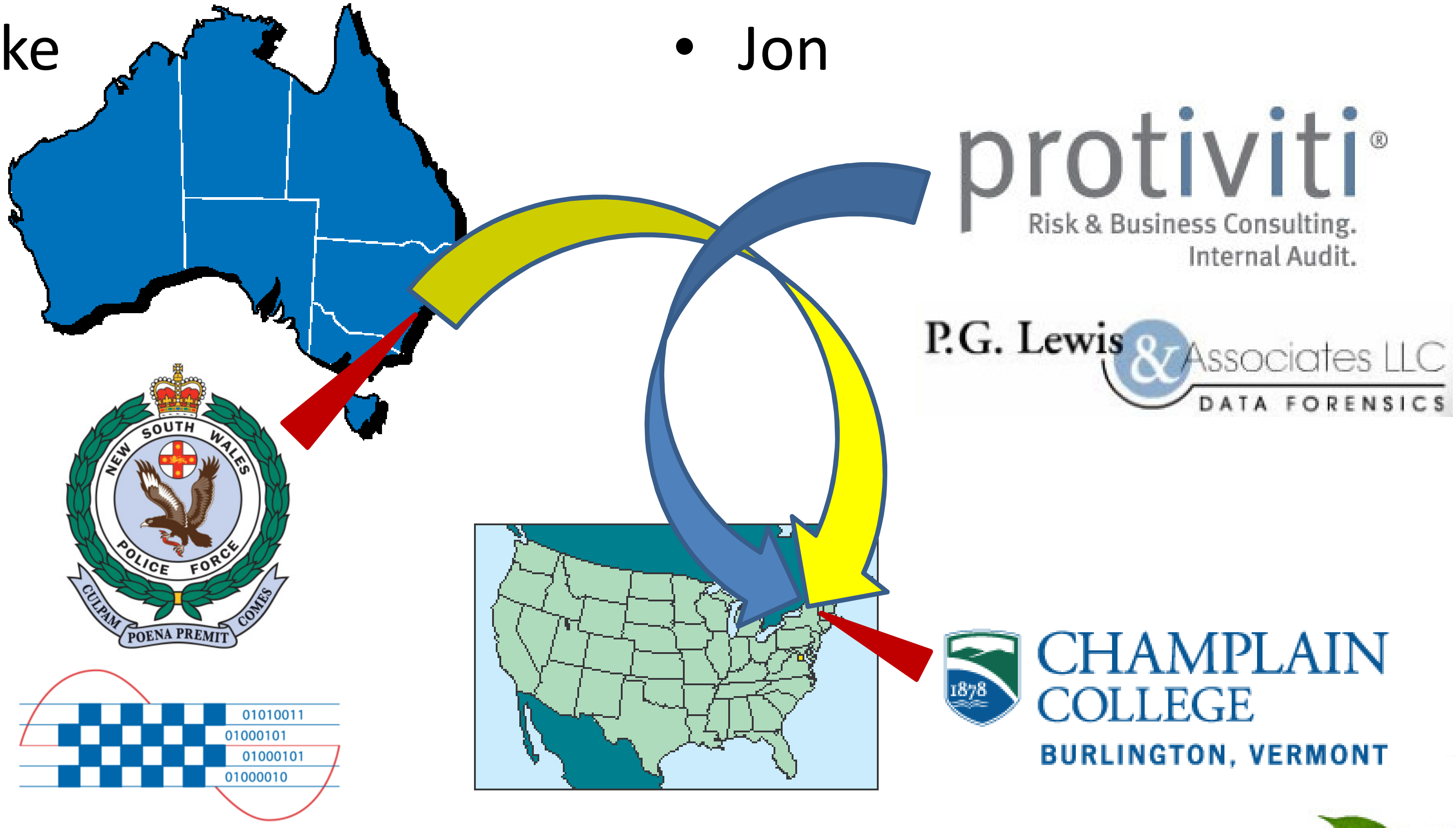
CEIC® 2011

Behavioral Analysis of Windows® Applications

Jonathan Rajewski
Michael Wilkinson

About Us

- Mike
- Jon



Contact Information

Michael Wilkinson
wilkinson@champlain.edu

Jonathan Rajewski
rajewski@champlain.edu

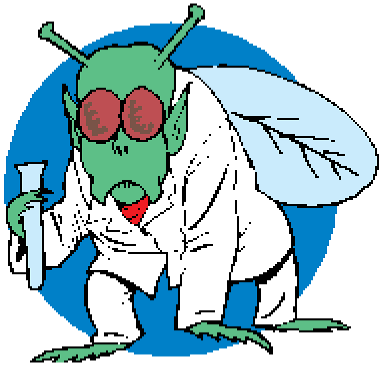
@jtrajewski

Overview

- Review methodology
- Observations
- Tools
- Hands on fun stuff (lab)

Today

Science + Windows + Dropbox



Starting Windows

© Microsoft Corporation

The Science

Scientific Method

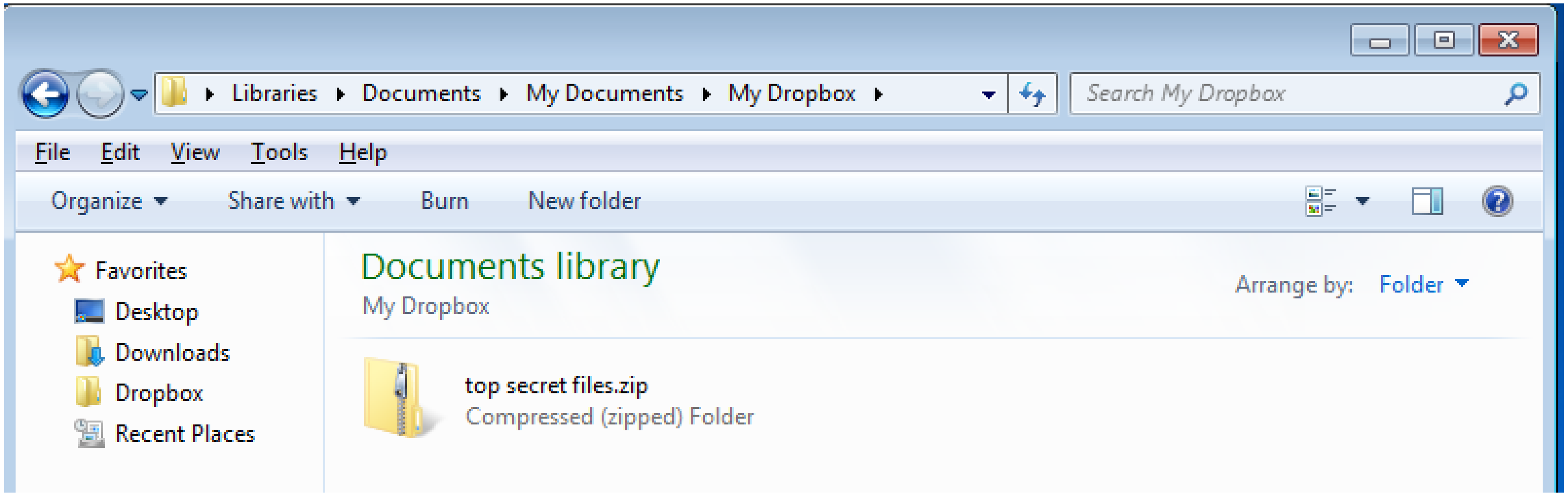
1. Define the question/problem
2. Information Collection
3. Develop theory
4. Test theory
5. Analyze results

Document

6 to 10….. peer review, publish, retest, refine

Scenario

Has this file been uploaded to Dropbox?



Libraries ▸ Documents ▸ My Documents ▸ My Dropbox ▸

Documents library

My Dropbox

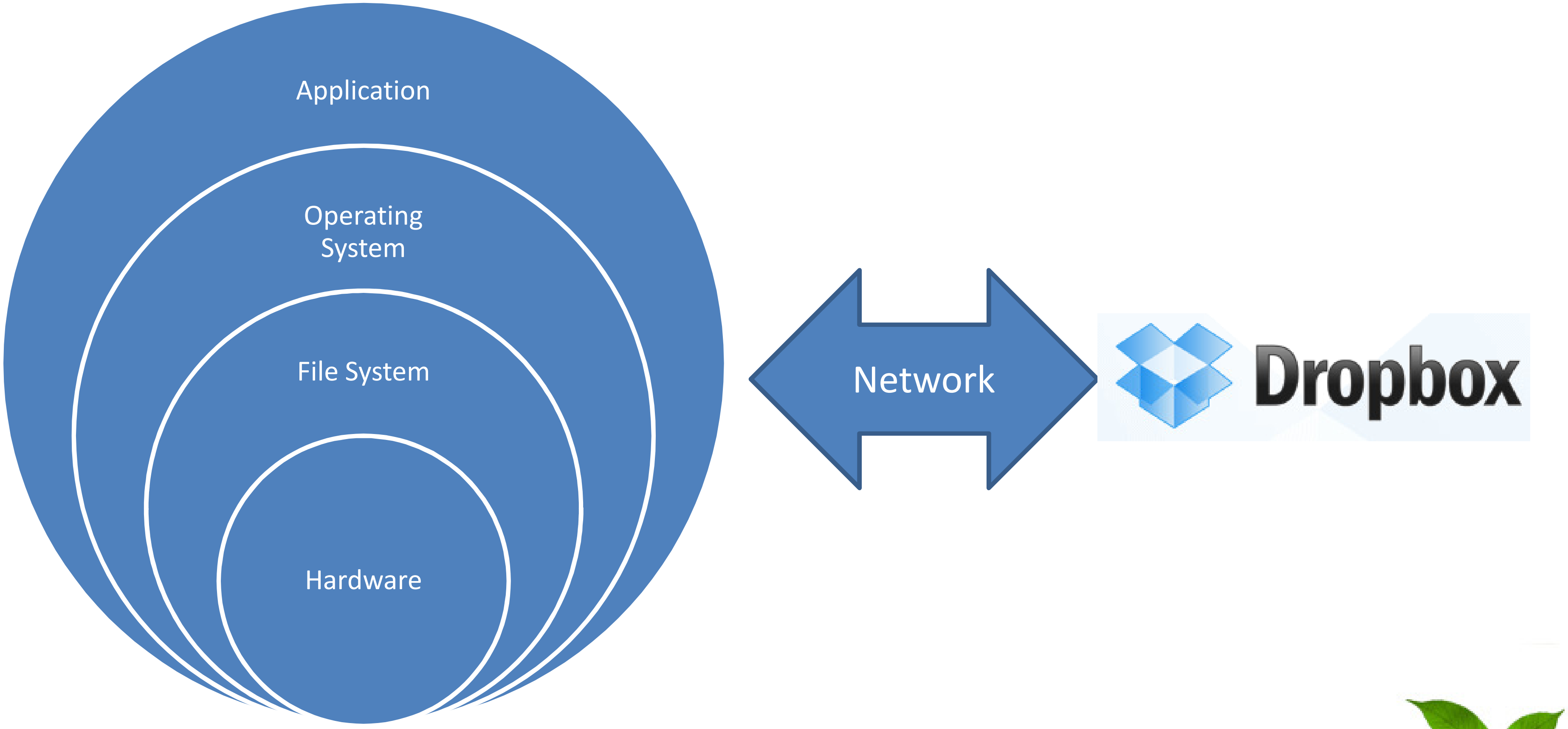
top secret files.zip

Compressed (zipped) Folder

- Where was it installed
- What happens when the user installs it
- Functionality
- Capability

http://blog.futurewomenleaders.net/Portals/40552/images%5C/goal-sm.jpg

Observation

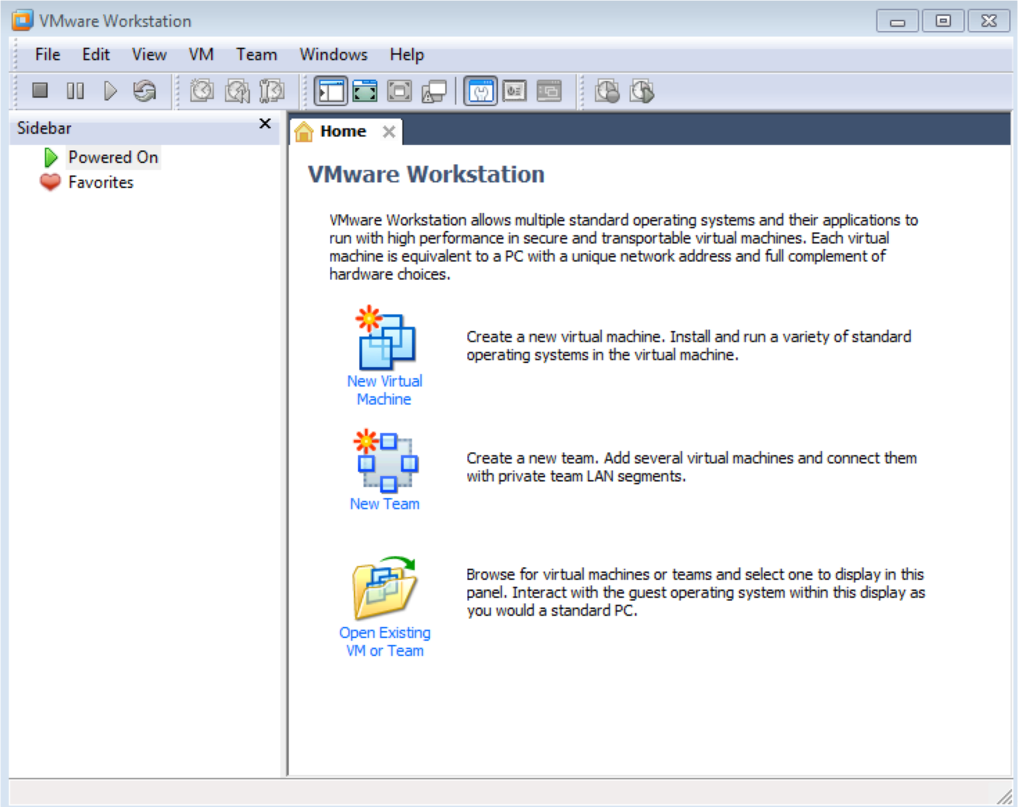


Tools

Virtual Machines

CEIC® 2011

An excellent way to quickly test an applications behavior



VMware Workstation

VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.

Create a new virtual machine. Install and run a variety of standard operating systems in the virtual machine.

Create a new team. Add several virtual machines and connect them with private team LAN segments.

Browse for virtual machines or teams and select one to display in this panel. Interact with the guest operating system within this display as you would a standard PC.

Process Monitor

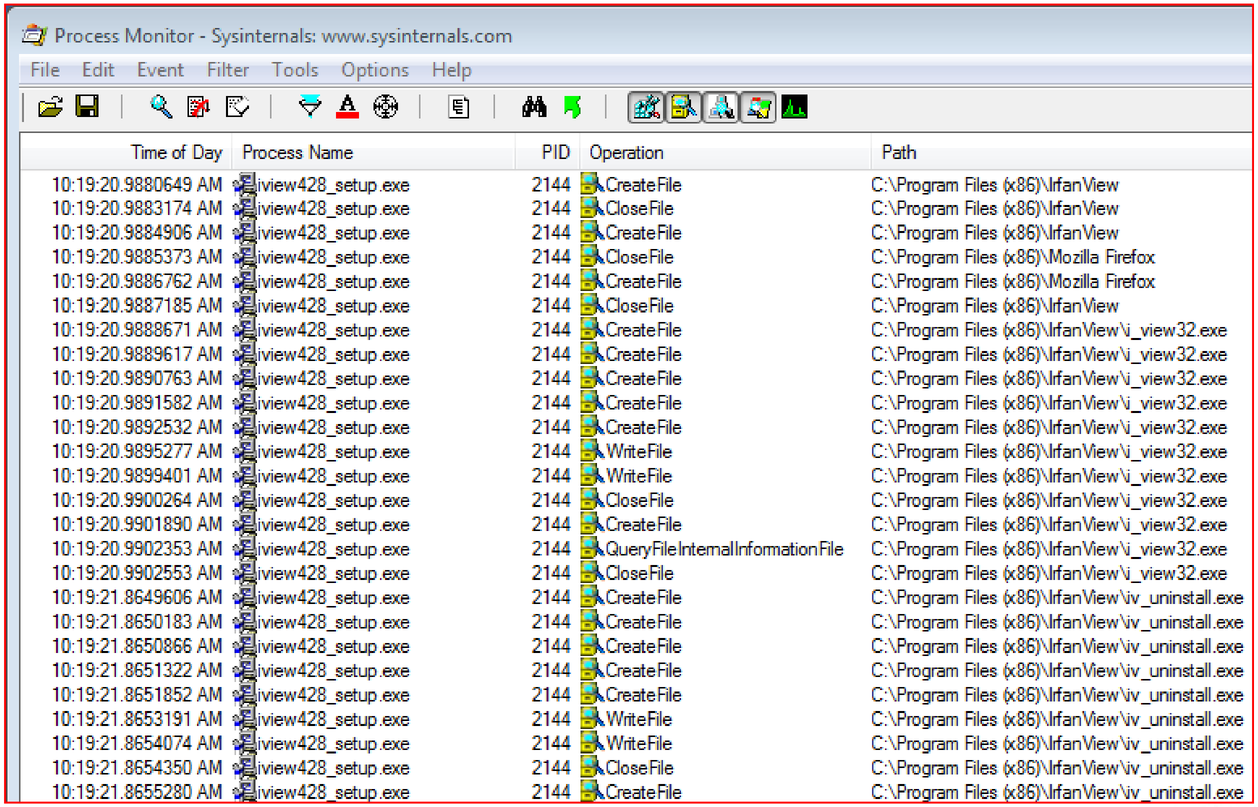
- Testing Environment (VM)
  - – Use Process Monitor (Sysinternals)

Process Monitor v2.95

By Mark Russinovich and Bryce Cogswell

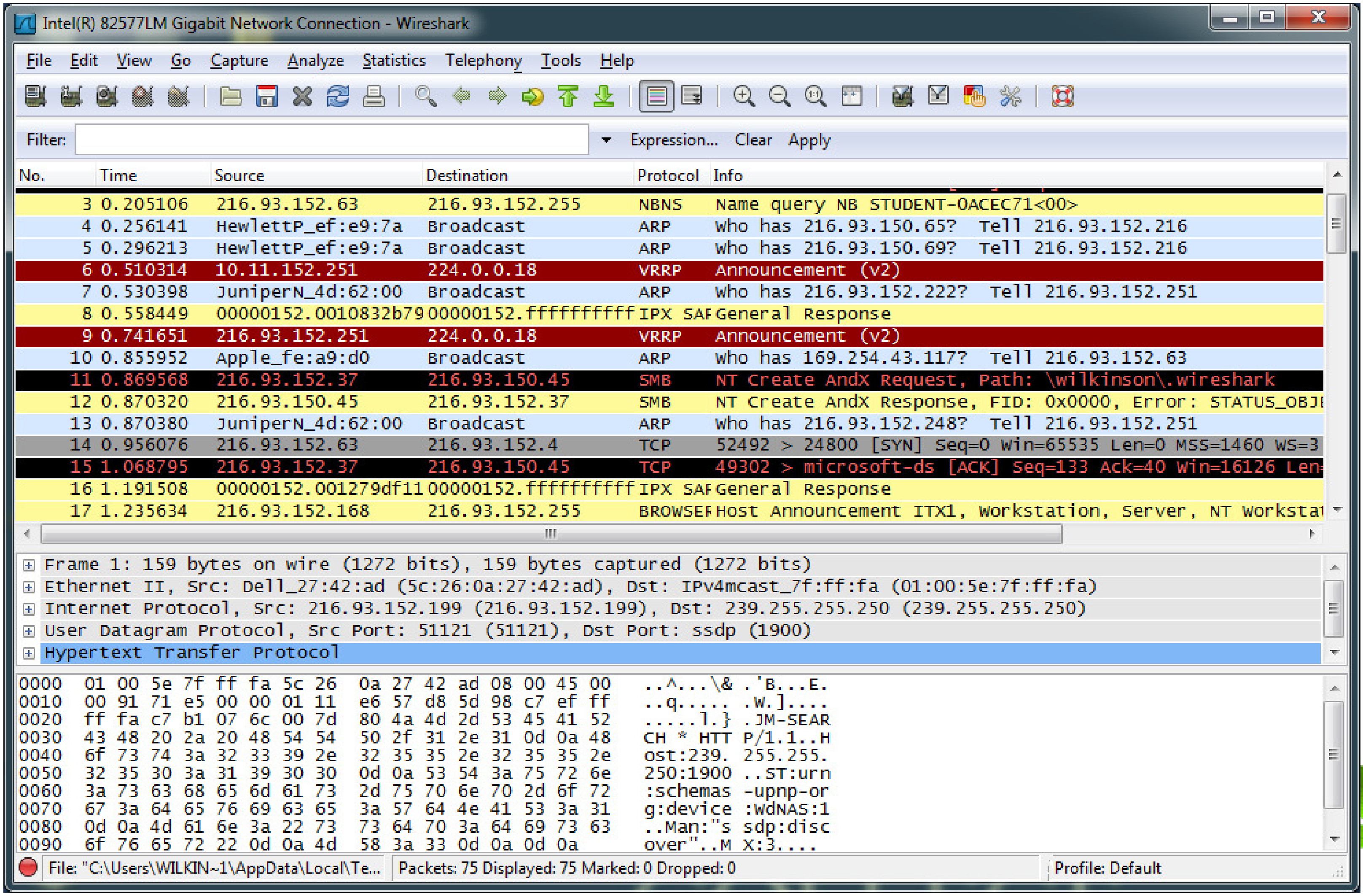
Published: April 13, 2011

Download Process Monitor (1.26 MB)


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path
10:19:20.9880649 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView
10:19:20.9883174 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\IrfanView
10:19:20.9884906 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView
10:19:20.9885373 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\Mozilla Firefox
10:19:20.9886762 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\Mozilla Firefox
10:19:20.9887185 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\IrfanView
10:19:20.9888671 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9889617 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9890763 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9891582 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9892532 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9895277 AM	iview428_setup.exe	2144	WriteFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9899401 AM	iview428_setup.exe	2144	WriteFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9900264 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9901890 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9902353 AM	iview428_setup.exe	2144	QueryFileInternalInformationFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:20.9902553 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\IrfanView\i_view32.exe
10:19:21.8649606 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8650183 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8650866 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8651322 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8651852 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8653191 AM	iview428_setup.exe	2144	WriteFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8654074 AM	iview428_setup.exe	2144	WriteFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8654350 AM	iview428_setup.exe	2144	CloseFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe
10:19:21.8655280 AM	iview428_setup.exe	2144	CreateFile	C:\Program Files (x86)\IrfanView\iv_uninstall.exe

Wireshark



```
No.    Time      Source               Destination          Protocol  Info
     3 0.205106  216.93.152.63        216.93.152.255       NBNS      Name query NB STUDENT-0ACEC71<00>
     4 0.256141  HewlettP_ef:e9:7a    Broadcast            ARP       Who has 216.93.150.65?  Tell 216.93.152.216
     5 0.296213  HewlettP_ef:e9:7a    Broadcast            ARP       Who has 216.93.150.69?  Tell 216.93.152.216
     6 0.510314  10.11.152.251        224.0.0.18           VRRP      Announcement (v2)
     7 0.530398  JuniperN_4d:62:00    Broadcast            ARP       Who has 216.93.152.222?  Tell 216.93.152.251
     8 0.558449  00000152.0010832b79 00000152.ffffffffff IPX SAF  General Response
     9 0.741651  216.93.152.251       224.0.0.18           VRRP      Announcement (v2)
    10 0.855952  Apple_fe:a9:d0       Broadcast            ARP       Who has 169.254.43.117?  Tell 216.93.152.63
    11 0.869568  216.93.152.37        216.93.150.45        SMB       NT Create AndX Request, Path: \wilkinson\.wireshark
    12 0.870320  216.93.150.45        216.93.152.37        SMB       NT Create AndX Response, FID: 0x0000, Error: STATUS_OBJE
    13 0.870380  JuniperN_4d:62:00    Broadcast            ARP       Who has 216.93.152.248?  Tell 216.93.152.251
    14 0.956076  216.93.152.63        216.93.152.4         TCP       52492 > 24800 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3
    15 1.068795  216.93.152.37        216.93.150.45        TCP       49302 > microsoft-ds [ACK] Seq=133 Ack=40 Win=16126 Len=
    16 1.191508  00000152.001279df11 00000152.ffffffffff IPX SAF  General Response
    17 1.235634  216.93.152.168       216.93.152.255       BROWSER   Host Announcement ITX1, Workstation, Server, NT Workstat
```

```
⊞ Frame 1: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits)
⊞ Ethernet II, Src: Dell_27:42:ad (5c:26:0a:27:42:ad), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
⊞ Internet Protocol, Src: 216.93.152.199 (216.93.152.199), Dst: 239.255.255.250 (239.255.255.250)
⊞ User Datagram Protocol, Src Port: 51121 (51121), Dst Port: ssdp (1900)
⊞ Hypertext Transfer Protocol
```

```
0000  01 00 5e 7f ff fa 5c 26  0a 27 42 ad 08 00 45 00   ..^...\& .'B...E.
0010  00 91 71 e5 00 00 01 11  e6 57 d8 5d 98 c7 ef ff   ..q..... .W.]....
0020  ff fa c7 b1 07 6c 00 7d  80 4a 4d 2d 53 45 41 52   .....l.} .JM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1..H
0040  6f 73 74 3a 32 33 39 2e  32 35 35 2e 32 35 35 2e   ost:239. 255.255.
0050  32 35 30 3a 31 39 30 30  0d 0a 53 54 3a 75 72 6e   250:1900 ..ST:urn
0060  3a 73 63 68 65 6d 61 73  2d 75 70 6e 70 2d 6f 72   :schemas -upnp-or
0070  67 3a 64 65 76 69 63 65  3a 57 64 4e 41 53 3a 31   g:device :WdNAS:1
0080  0d 0a 4d 61 6e 3a 22 73  73 64 70 3a 64 69 73 63   ..Man:"s sdp:disc
0090  6f 76 65 72 22 0d 0a 4d  58 3a 33 0d 0a 0d 0a      over"..M X:3....
```

File: "C:\Users\WILKIN~1\AppData\Local\Te... | Packets: 75 Displayed: 75 Marked: 0 Dropped: 0 | Profile: Default

SQLite Manager

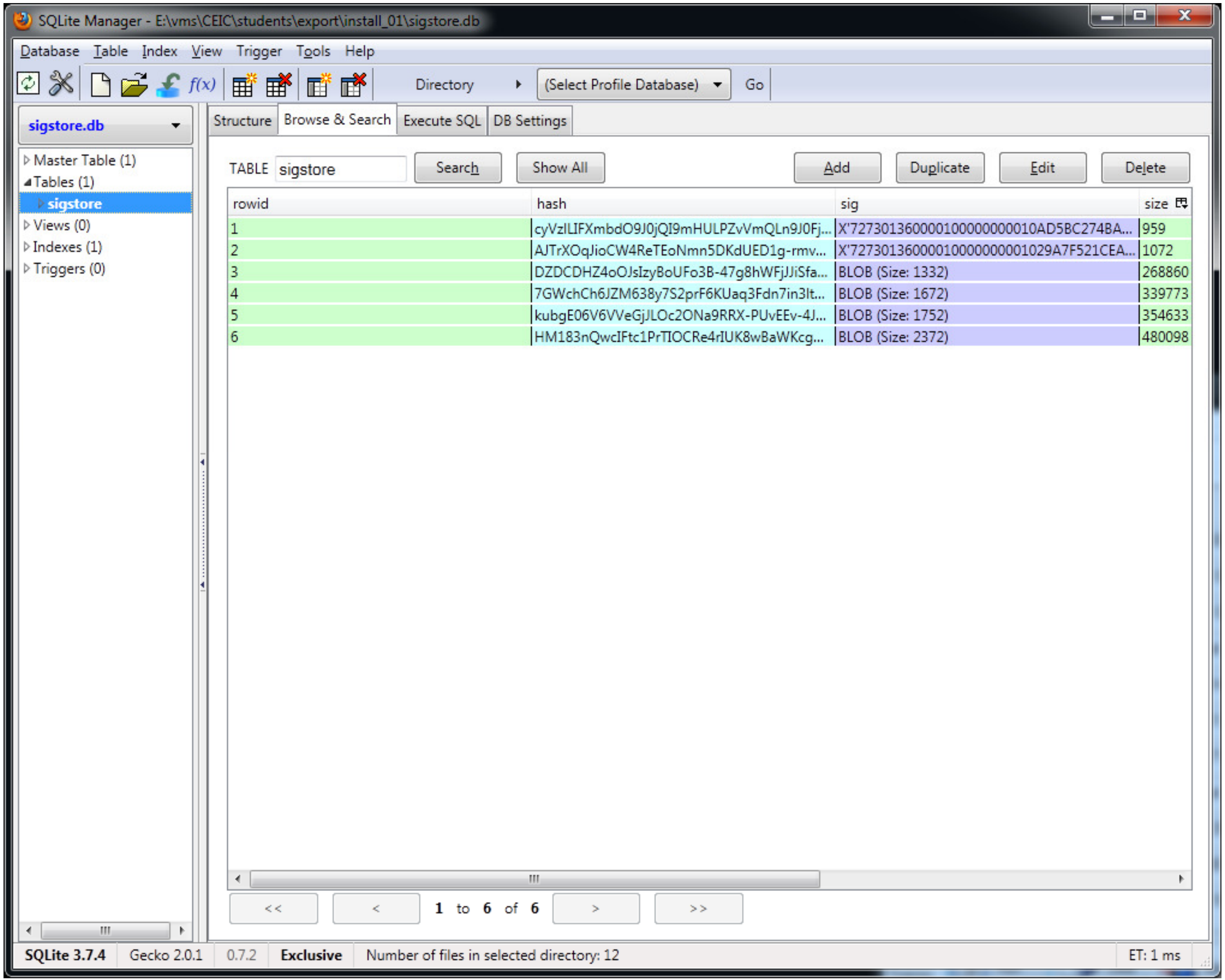


TABLE sigstore

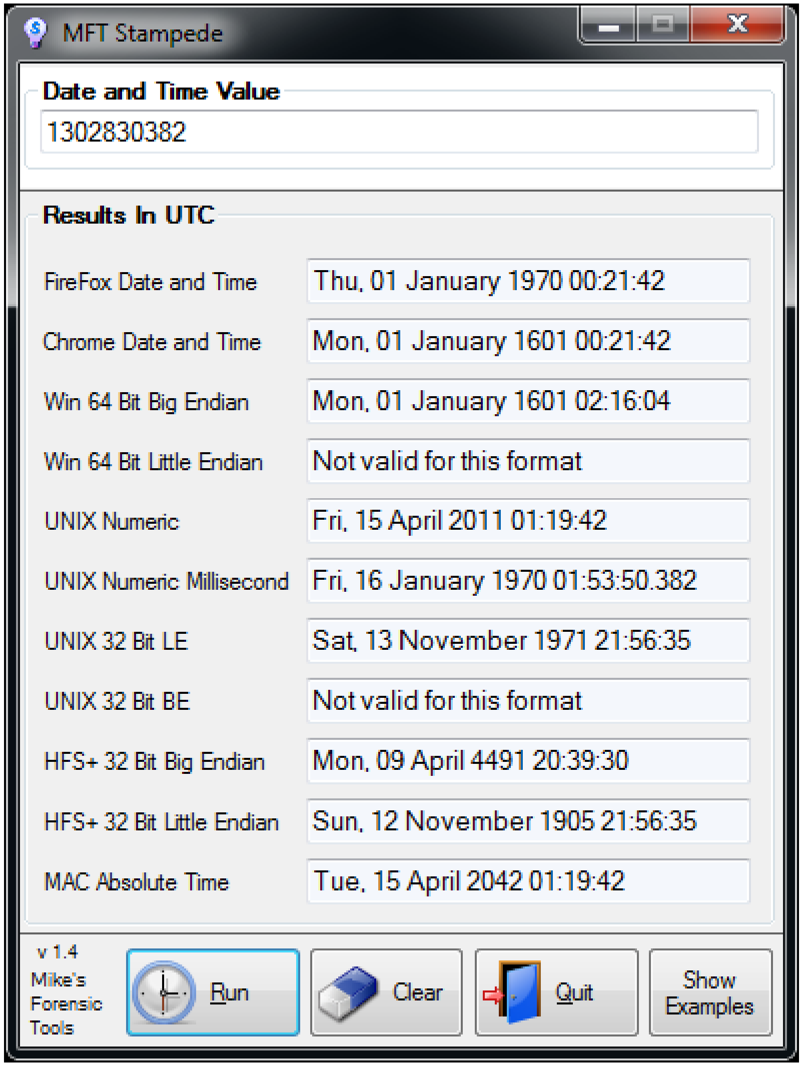
rowid	hash	sig	size
1	cyVzILIFXmbdO9J0jQI9mHULPZvVmQLn9J0Fj...	X'727301360000100000000010AD5BC274BA...	959
2	AJTrXOqJioCW4ReTEoNmn5DKdUED1g-rmv...	X'72730136000010000000001029A7F521CEA...	1072
3	DZDCDHZ4oOJsIzyBoUFo3B-47g8hWFjJJiSfa...	BLOB (Size: 1332)	268860
4	7GWchCh6JZM638y7S2prF6KUaq3Fdn7in3lt...	BLOB (Size: 1672)	339773
5	kubgE06V6VVeGjJLOc2ONa9RRX-PUvEEv-4J...	BLOB (Size: 1752)	354633
6	HM183nQwcIFtc1PrTIOCRe4rIUK8wBaWKcg...	BLOB (Size: 2372)	480098

1 to 6 of 6

Number of files in selected directory: 12

ET: 1 ms

MFT Stampede



Date and Time Value

1302830382

Results In UTC

FireFox Date and Time	Thu, 01 January 1970 00:21:42
Chrome Date and Time	Mon, 01 January 1601 00:21:42
Win 64 Bit Big Endian	Mon, 01 January 1601 02:16:04
Win 64 Bit Little Endian	Not valid for this format
UNIX Numeric	Fri, 15 April 2011 01:19:42
UNIX Numeric Millisecond	Fri, 16 January 1970 01:53:50.382
UNIX 32 Bit LE	Sat, 13 November 1971 21:56:35
UNIX 32 Bit BE	Not valid for this format
HFS+ 32 Bit Big Endian	Mon, 09 April 4491 20:39:30
HFS+ 32 Bit Little Endian	Sun, 12 November 1905 21:56:35
MAC Absolute Time	Tue, 15 April 2042 01:19:42

Good o'l Fashioned Forensic Work

Let’s talk about Dropbox…

Dropbox

FILES
FILES
FILES

Resources

- www.vmware.com
- www.wireshark.org
- technet.microsoft.com/en-us/sysinternals/bb896645
- code.google.com/p/sqlite-manager/
- http://www.mikesforensictools.co.uk/downloads.html