Incident Handling around the world in 80 ms.
(Well not really that fast…)

Steve Mancini

Greg Bassett

with special guest star…

Russ McRee

20th FIRST Annual Conference

VANCOUVER British Columbia
Canada June 22-27, 2008

Caveat

The opinions expressed in this presentation are those of the authors (or at least the one talking) and do not reflect the opinions of our employers.

Any resemblance to real persons living, dead or undead is purely coincidental.
No animals were harmed in the making of this presentation or program.
Any resemblance to any place in cyberspace is entirely coincidental.
No other warranty expressed or implied.
Contents may settle during shipment.
Void where prohibited by law.
Some assembly required.
Batteries not included.
Use only as directed.

Agenda

- Brief Explanation: What is RAPIER
- Establishing a RAPIER results repository
- Coffee Break
- RAPIER Module Writing 101
- Module Analysis Deep Dive
- Feature Requests / Feedback

IR 101

To avoid redundancy and for the sake of time we are avoiding explaining things:

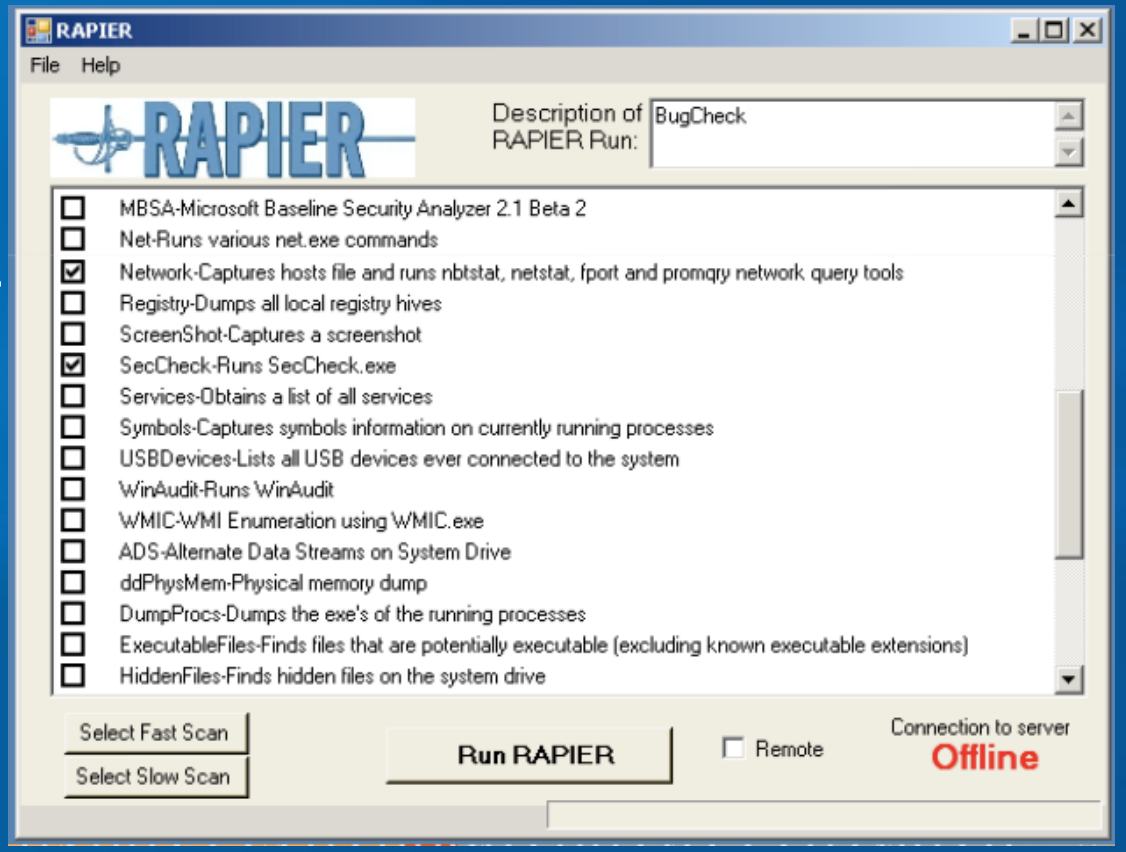
- Order of Volatility
- Definitions of “forensically sound”

Hopefully you all had the opportunity to attend Par’s and Russ’ presentation on Monday; they did a great job covering this content. Yes they stole my thunder ☺

WHAT IS RAPIER

RAPIER

- Modular
- Stand Alone
- Client / Server
- Automated
- Configurable
- Expandable
- CLI
- FREE



Why would I need it?

- The worst time to learn how to acquire information from a system is *during the incident.*
- Expertise does not scale (to most enterprise environments)
- Not everyone knows how to acquire the requested information
- Not everyone acquires it in the same fashion
- Common (1st) responses may trample valuable information
  - Run Scanners, Patch System, Update Apps

RAPIER Output

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

“Forensically Sound?”

Topic has come up.

Some say yes…

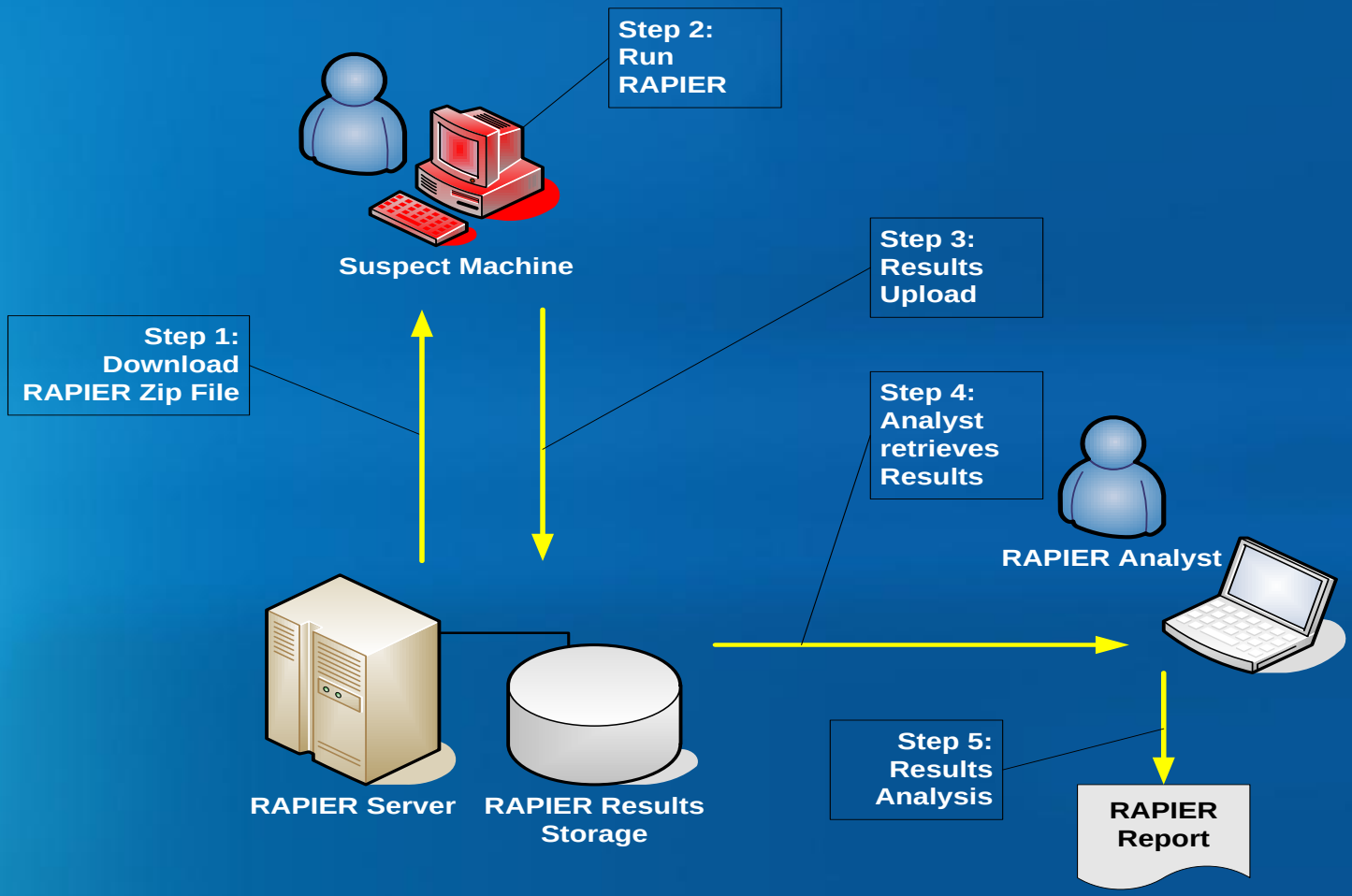
Some say no…

Some say HELL NO!

“Forensics Integrity Check” option exists.

RAPIER SERVER

RAPIER Workflow



Considerations

- Audience has fundamental understanding of system administration and web server setup is assumed…
- Non-denominational OS Disclaimer
  - The following configuration focuses on a Windows server running WAMP
  - Does **not** have to be Windows/WAMP!
  - Web server **is** necessary (WAMP, LAMP, IIS)
  - Web written in PHP, can be done in .NET
- Web Server with at least 20GB

Storage

- RAPIER results size depends on modules run
  - Average Fast Scan dump ~ 15MB
  - Add File capture, WebCache ~ 1GB
  - Physical Memory Dump – size of memory - ~1 GB+
  - Recommend at least 20 GB for typical usage
  - Need to size according to site use
- Website
  - Small size ~300 MB
  - RAPIER executables, web support files

Access

- RAPIER_Analysts group access to RAPIER_Results directory
- RAPIER_Dev group access for module configs and updates

Notifications

- Client and Server utilize blat to send email
- RAPIER Results Notification
  - Sent from Client, configured in RAPIER.conf
  - Notification that Results file was uploaded
- Upload Notification
  - Sent from Server, configured in index.php
  - Notification that Malware sample was uploaded

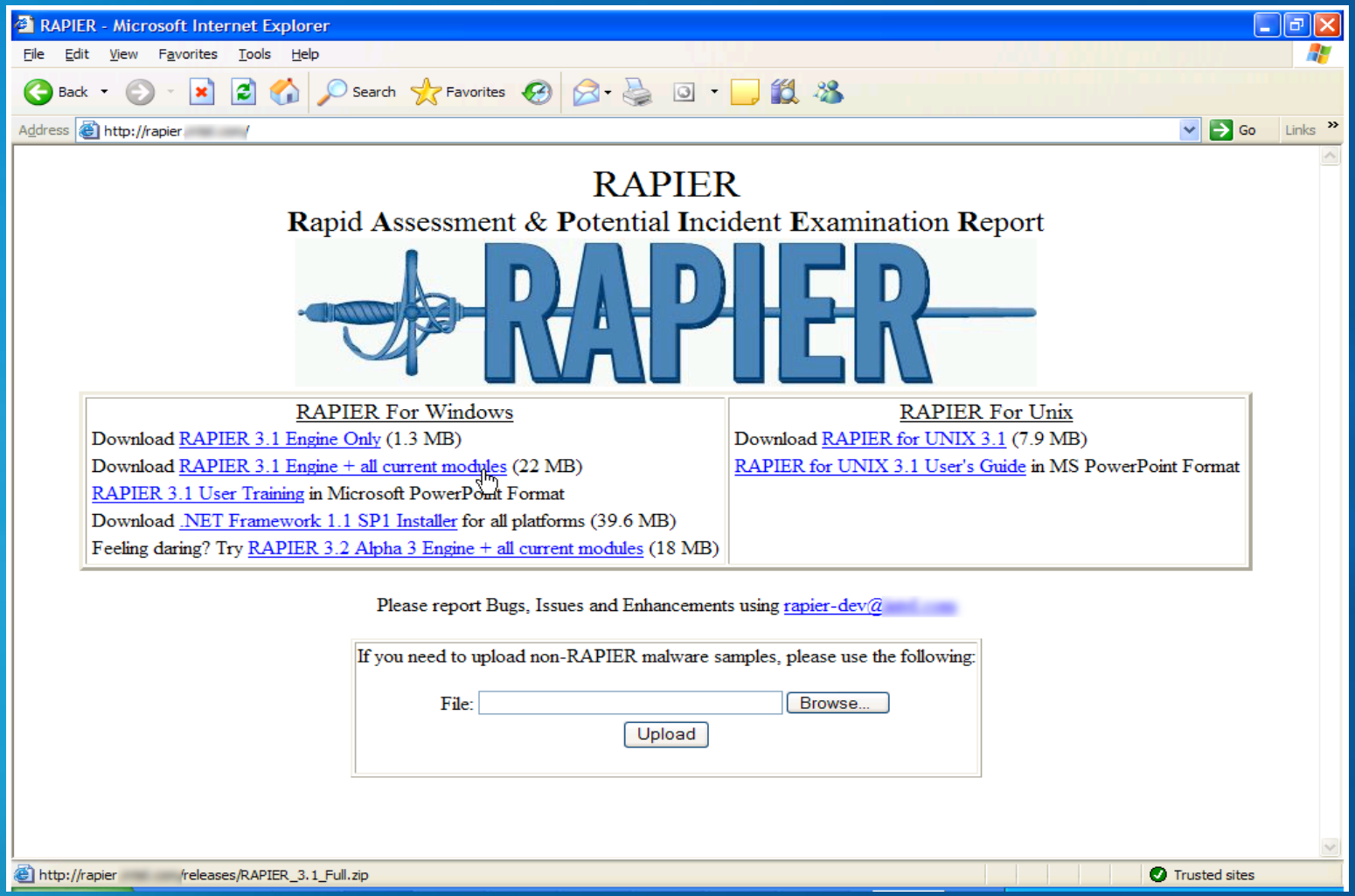
Firewall

- Web server
  - Port 80 – RAPIER Zip download
  - Defined port (8010) – RAPIER to server communications (Results file upload)
    - Separate port configured to provide functionality during port 80 malware outbreak
- Results
  - File share- port 445
  - SFTP- port 22
- Notifications
  - SMTP- port 25
- RDP
  - Port 3389

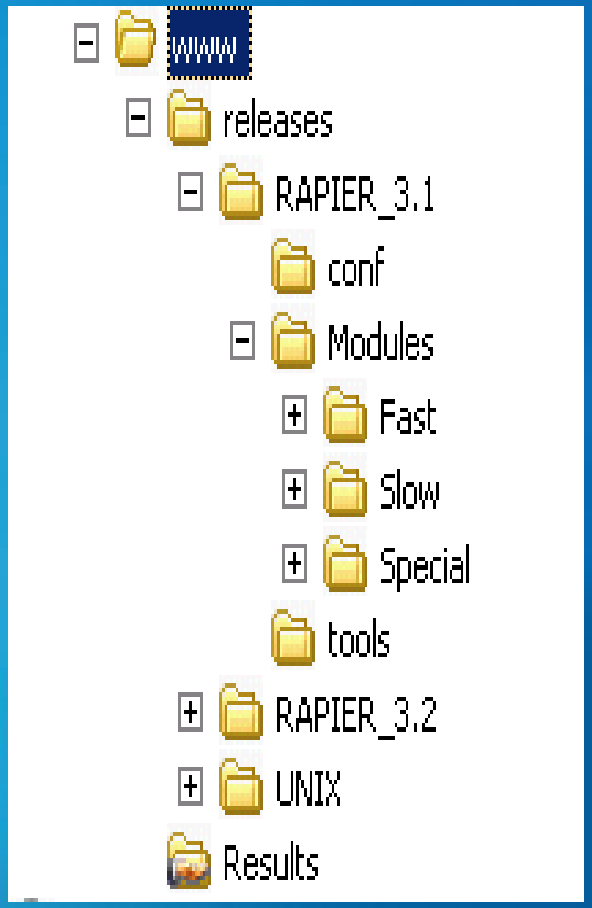
Web Functionality

- RAPIER Zip File
  - Provides download of Zip file
- RAPIER User guides
  - Provides download of User guides
- RAPIER Results Uploads
  - Provides upload support to RAPIER_Results
- Sample Uploads
  - Provides upload support for Malware found during RAPIER analysis

Web Site



Web Site Directory Structure



Name	Size	Type
releases		File Folder
Results		File Folder
7za.exe	478 KB	Application
blat.exe	94 KB	Application
blat.log	11 KB	Text Document
checksum.php	5 KB	PHP File
CurrentVersionSHA1.txt	1 KB	Text Document
DotNetFW_Install.zip	40,512 KB	WinZip File
GenerateFullZIP.cmd	1 KB	Windows Command ...
GenerateFullZIP.vbs	16 KB	VBScript Script File
index.php	13 KB	PHP File
RAPIER 3.1 User Training.ppt	691 KB	PPT File
RAPIER 3.2 Server Setup.txt	4 KB	Text Document
RAPIER 3.2 User Training.ppt	721 KB	PPT File
RAPIER for UNIX 3.1 Users Guide.ppt	513 KB	PPT File
RAPIER.jpg	14 KB	JPEG Image
sha1sum.exe	54 KB	Application
test.html	1 KB	HTML Document
version.php	2 KB	PHP File

Web Server Setup

- Install Web Server
- Install RAPIER Web Site
- Create/Share Results directory
- Configure Web Server
- Configure RAPIER
- Scheduled Tasks
- Testing

Web Server/Site Install

- Install WAMP/LAMP/IIS
  - WAMP5 Server 1.7.x or newer
  - MySQL is disabled!
- Install RAPIER Web site files
  - Web page, releases, user guides

Results Directory

- Create results directory
  - D:\wamp\www\RAPIER_results
- Configure access\sharing for RAPIER_Analysts
  - Windows File Sharing
  - Secure FTP
  - Secure Web hosting /directory browsing enabled

Configure httpd.conf

- Listening Ports
  - "Listen" line includes port 80 and port 8010
- Add results directory paths below web root
  - Alias /results "D:/wamp/www/results"
  - <Directory "D:/wamp/www/results">
- Change Web Root defaults
  - Allow/Deny for the web root to "Allow from all"
  - Remove "Indexes“
- DAV Support
  - Uncomment the following two modules:
    - LoadModule dav_module modules/mod_dav.so
    - LoadModule dav_fs_module modules/mod_dav_fs.so

Configure index.php

- Target Path
  - $target_path="d:\\wamp\\www\\Results";
- SMTP Server
  - $StrSMTPServer="*my.smtp.server*";
- Upload Notifications
  - $StrEmailAddressFrom="Malware.Samples@myorg";
  - $StrEmailAddressTo="RAPIER.Results.Notifications@myorg";
  - $StrEmailAddressCC="";
  - $StrEmailAddressBCC="";
  - $StrSubject="Malware Sample Upload Notification";
- Embedded Notification Information
  - $StrSampleLocation="*RAPIERServer*\\RAPIER_Results\\";
  - $StrHelpContact="";

Configure RAPIER.conf

- Configuration of RAPIER.conf on server copy
  - Zip file created for distribution
- URLs
  - Define Base URL
    - RAPIERBaseURL=http://*RAPIERURL*:8010
  - Define Results URL
    - UploadURL=<RAPIERBaseURL>/Results/
- SMTP Server
  - Define SMTP server
    - SMTPServer=*my.smtp.server*

Cont'd

- Results Notifications
  - Required values
    - EmailFrom=RAPIER.Results@*myorg*
    - EmailTo=RAPIER.Results.Notification@*myorg*
      - *EmailTo needs to be a valid address*
  - Optional values
    - EmailCC=
    - EmailBCC=
- Embedded Results Information
  - Where results were loaded
    - SampleLocation=*RAPIERServer*\RAPIER_Results\
  - Who to contact for help
    - HelpContact=

Configure proxy.conf

- Modules that require a connection to the network
- AutoProxyURL=http://autoproxy:*nnnn*
- ProxyServer=proxy:*nnn*

Scheduled Tasks

- Need to keep AV DAT and MBSA CAB files updated
  - Modules\Special\ClamAVScan\Module.cmd updateDATonly – 2 hours
  - Modules\Special\McAfeeVirusScan\Module.cmd updateDATonly" - 2 hours
  - Modules\Fast\MBSA\Module.cmd updateCABonly" – Daily
- Need to keep RAPIER Zip file current
  - GenerateFullZIP.cmd – 10 minutes

Cont'd

- Results share
  - Determine policy/retention time for results
- Monitor Scheduled tasks
  - Tasks run as required- DATs get updated
- Other Server tasks
  - Monitor disk space, server availability
  - Patching, etc

Server Testing

- http://*RAPIERserver* – URL available?
  - Web server running, port blocked?
- Download RAPIER ZIP
  - ZIP file in releases directory?
- Run RAPIER with a few modules- runs with no errors?
  - Check .Net package, files extracted from ZIP
- Results upload with no errors
  - Web Server configuration
- Verify Results email – results email received?
  - SMTP/Notification settings, port blocked?
- Scheduled Tasks – do they run?
  - Proxy settings

Digression

MODULE CREATION

Module Architecture

- Based on VBScript
- RAPIER.vbi is a large library of VBScript functions to reference
- Modules can have individual conf files to allow for end user configuration
- Modules are stand alone
  - Can be added/removed/modified at will
  - Allows for independent development/testing

Module Creation

1. Find a cool tool you want to incorporate
2. Understand that tool's CLI
3. Wrap
4. Test
5. Incorporate

C:\Windows\Prefetch

A lot of discussions about prefetch lately.

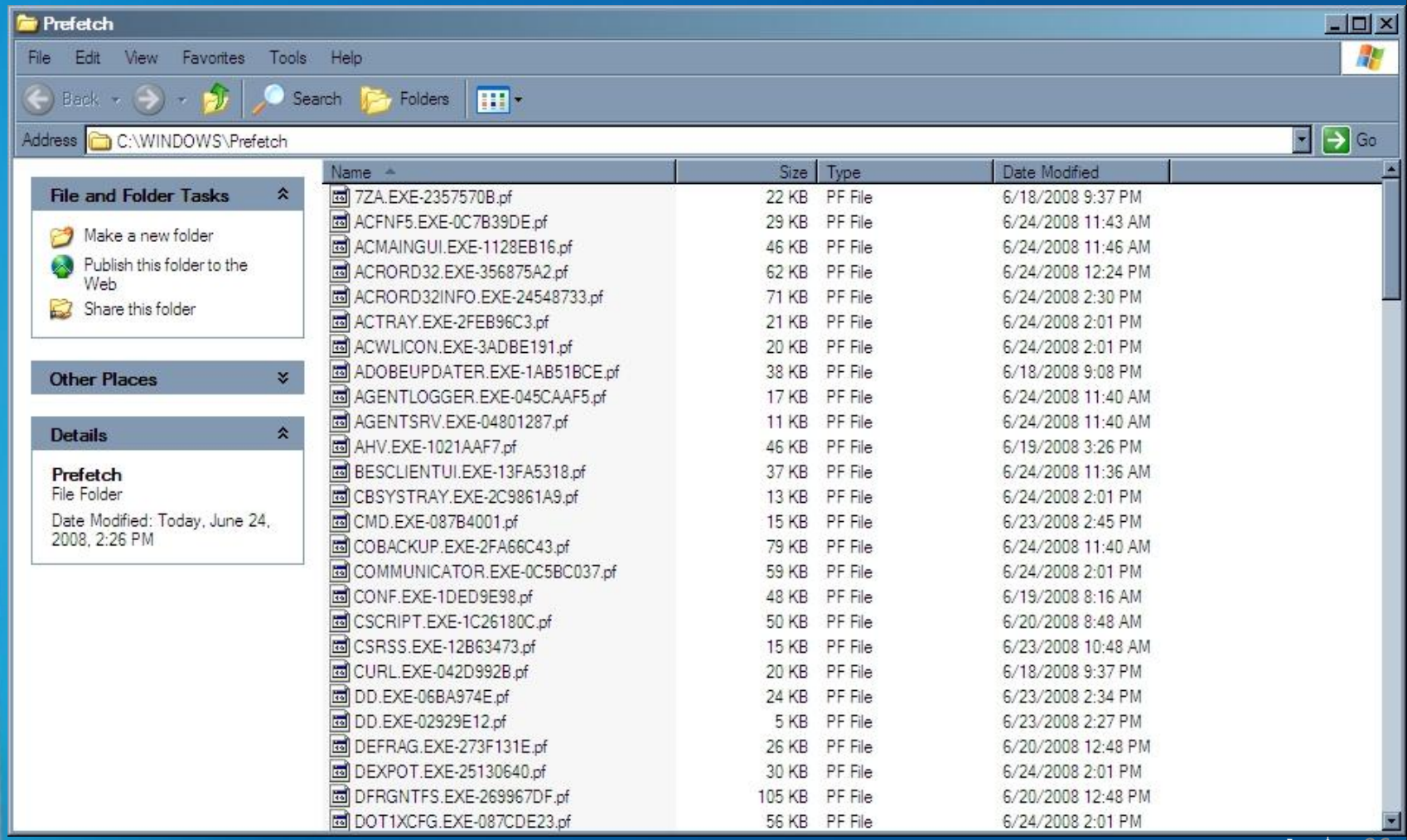
Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need…

C:\Windows\Prefetch



C:\Windows\Prefetch

A lot of discussions about prefetch lately.

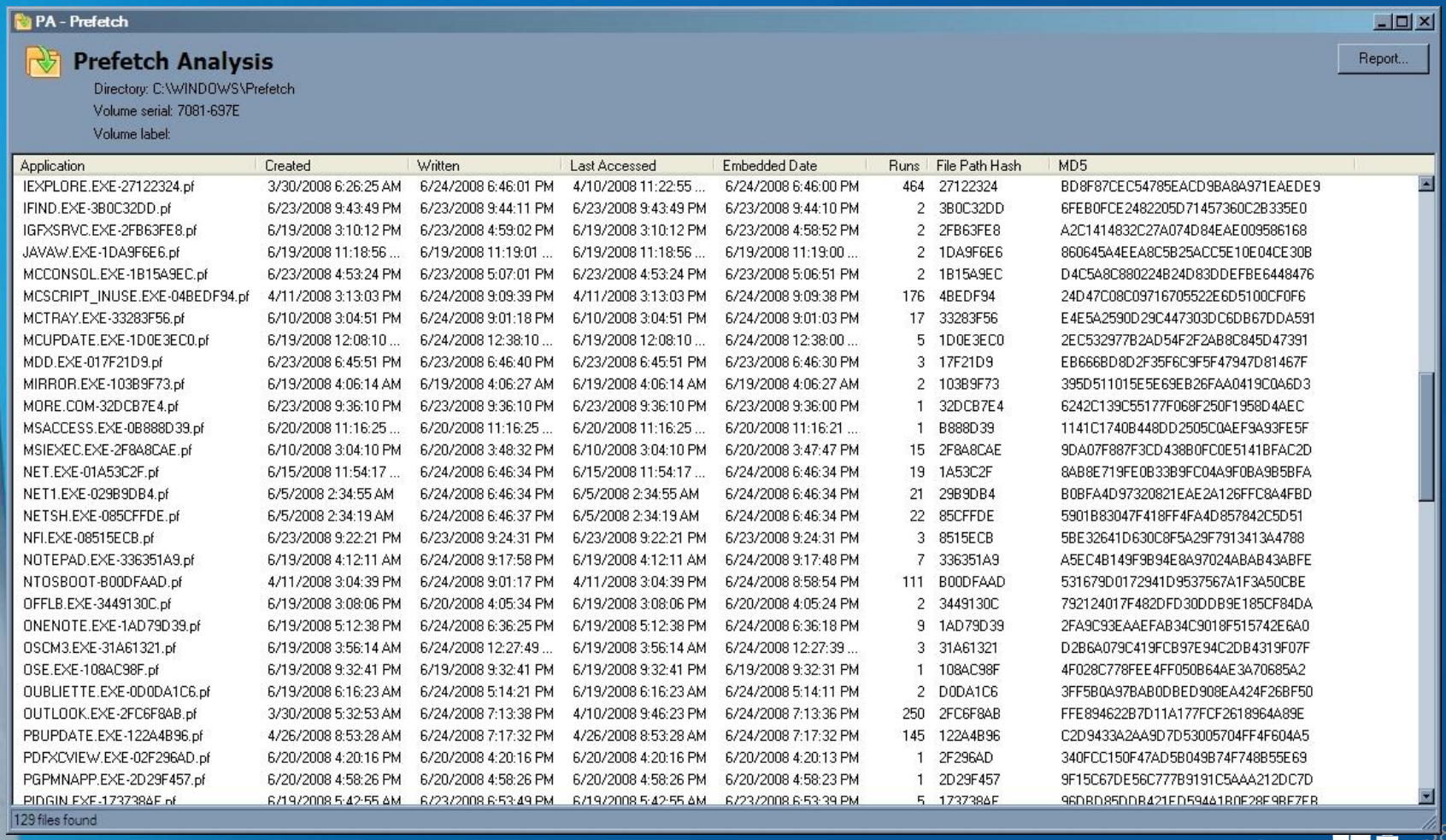
Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need…

C:\Windows\Prefetch



Application	Created	Written	Last Accessed	Embedded Date	Runs	File Path Hash	MD5
IEXPLORE.EXE-27122324.pf	3/30/2008 6:26:25 AM	6/24/2008 6:46:01 PM	4/10/2008 11:22:55 ...	6/24/2008 6:46:00 PM	464	27122324	BD8F87CEC54785EACD9BA8A971EAEDE9
IFIND.EXE-3B0C32DD.pf	6/23/2008 9:43:49 PM	6/23/2008 9:44:11 PM	6/23/2008 9:43:49 PM	6/23/2008 9:44:10 PM	2	3B0C32DD	6FEB0FCE2482205D71457360C2B335E0
IGFXSRVC.EXE-2FB63FE8.pf	6/19/2008 3:10:12 PM	6/23/2008 4:59:02 PM	6/19/2008 3:10:12 PM	6/23/2008 4:58:52 PM	2	2FB63FE8	A2C1414832C27A074D84EAE009586168
JAVAW.EXE-1DA9F6E6.pf	6/19/2008 11:18:56 ...	6/19/2008 11:19:01 ...	6/19/2008 11:18:56 ...	6/19/2008 11:19:00 ...	2	1DA9F6E6	860645A4EEA8C5B25ACC5E10E04CE30B
MCCONSOL.EXE-1B15A9EC.pf	6/23/2008 4:53:24 PM	6/23/2008 5:07:01 PM	6/23/2008 4:53:24 PM	6/23/2008 5:06:51 PM	2	1B15A9EC	D4C5A8C880224B24D83DDEFBE6448476
MCSCRIPT_INUSE.EXE-04BEDF94.pf	4/11/2008 3:13:03 PM	6/24/2008 9:09:39 PM	4/11/2008 3:13:03 PM	6/24/2008 9:09:38 PM	176	4BEDF94	24D47C08C09716705522E6D5100CF0F6
MCTRAY.EXE-33283F56.pf	6/10/2008 3:04:51 PM	6/24/2008 9:01:18 PM	6/10/2008 3:04:51 PM	6/24/2008 9:01:03 PM	17	33283F56	E4E5A2590D29C447303DC6DB67DDA591
MCUPDATE.EXE-1D0E3EC0.pf	6/19/2008 12:08:10 ...	6/24/2008 12:38:10 ...	6/19/2008 12:08:10 ...	6/24/2008 12:38:00 ...	5	1D0E3EC0	2EC532977B2AD54F2F2AB8C845D47391
MDD.EXE-017F21D9.pf	6/23/2008 6:45:51 PM	6/23/2008 6:46:40 PM	6/23/2008 6:45:51 PM	6/23/2008 6:46:30 PM	3	17F21D9	EB666BD8D2F35F6C9F5F47947D81467F
MIRROR.EXE-103B9F73.pf	6/19/2008 4:06:14 AM	6/19/2008 4:06:27 AM	6/19/2008 4:06:14 AM	6/19/2008 4:06:27 AM	2	103B9F73	395D511015E5E69EB26FAA0419C0A6D3
MORE.COM-32DCB7E4.pf	6/23/2008 9:36:10 PM	6/23/2008 9:36:10 PM	6/23/2008 9:36:10 PM	6/23/2008 9:36:00 PM	1	32DCB7E4	6242C139C55177F068F250F1958D4AEC
MSACCESS.EXE-0B888D39.pf	6/20/2008 11:16:25 ...	6/20/2008 11:16:25 ...	6/20/2008 11:16:25 ...	6/20/2008 11:16:21 ...	1	B888D39	1141C1740B448DD2505C0AEF9A93FE5F
MSIEXEC.EXE-2F8A8CAE.pf	6/10/2008 3:04:10 PM	6/20/2008 3:48:32 PM	6/10/2008 3:04:10 PM	6/20/2008 3:47:47 PM	15	2F8A8CAE	9DA07F887F3CD438B0FC0E5141BFAC2D
NET.EXE-01A53C2F.pf	6/15/2008 11:54:17 ...	6/24/2008 6:46:34 PM	6/15/2008 11:54:17 ...	6/24/2008 6:46:34 PM	19	1A53C2F	8AB8E719FE0B33B9FC04A9F0BA9B5BFA
NET1.EXE-029B9DB4.pf	6/5/2008 2:34:55 AM	6/24/2008 6:46:34 PM	6/5/2008 2:34:55 AM	6/24/2008 6:46:34 PM	21	29B9DB4	B0BFA4D97320821EAE2A126FFC8A4FBD
NETSH.EXE-085CFFDE.pf	6/5/2008 2:34:19 AM	6/24/2008 6:46:37 PM	6/5/2008 2:34:19 AM	6/24/2008 6:46:34 PM	22	85CFFDE	5901B83047F418FF4FA4D857842C5D51
NFI.EXE-08515ECB.pf	6/23/2008 9:22:21 PM	6/23/2008 9:24:31 PM	6/23/2008 9:22:21 PM	6/23/2008 9:24:31 PM	3	8515ECB	5BE32641D630C8F5A29F7913413A4788
NOTEPAD.EXE-336351A9.pf	6/19/2008 4:12:11 AM	6/24/2008 9:17:58 PM	6/19/2008 4:12:11 AM	6/24/2008 9:17:48 PM	7	336351A9	A5EC4B149F9B94E8A97024ABAB43ABFE
NTOSBOOT-B00DFAAD.pf	4/11/2008 3:04:39 PM	6/24/2008 9:01:17 PM	4/11/2008 3:04:39 PM	6/24/2008 8:58:54 PM	111	B00DFAAD	531679D0172941D9537567A1F3A50CBE
OFFLB.EXE-3449130C.pf	6/19/2008 3:08:06 PM	6/20/2008 4:05:34 PM	6/19/2008 3:08:06 PM	6/20/2008 4:05:24 PM	2	3449130C	792124017F482DFD30DDB9E185CF84DA
ONENOTE.EXE-1AD79D39.pf	6/19/2008 5:12:38 PM	6/24/2008 6:36:25 PM	6/19/2008 5:12:38 PM	6/24/2008 6:36:18 PM	9	1AD79D39	2FA9C93EAAEFAB34C9018F515742E6A0
OSCM3.EXE-31A61321.pf	6/19/2008 3:56:14 AM	6/24/2008 12:27:49 ...	6/19/2008 3:56:14 AM	6/24/2008 12:27:39 ...	3	31A61321	D2B6A079C419FCB97E94C2DB4319F07F
OSE.EXE-108AC98F.pf	6/19/2008 9:32:41 PM	6/19/2008 9:32:41 PM	6/19/2008 9:32:41 PM	6/19/2008 9:32:31 PM	1	108AC98F	4F028C778FEE4FF050B64AE3A70685A2
OUBLIETTE.EXE-0D0DA1C6.pf	6/19/2008 6:16:23 AM	6/24/2008 5:14:21 PM	6/19/2008 6:16:23 AM	6/24/2008 5:14:11 PM	2	D0DA1C6	3FF5B0A97BAB0DBED908EA424F26BF50
OUTLOOK.EXE-2FC6F8AB.pf	3/30/2008 5:32:53 AM	6/24/2008 7:13:38 PM	4/10/2008 9:46:23 PM	6/24/2008 7:13:36 PM	250	2FC6F8AB	FFE894622B7D11A177FCF2618964A89E
PBUPDATE.EXE-122A4B96.pf	4/26/2008 8:53:28 AM	6/24/2008 7:17:32 PM	4/26/2008 8:53:28 AM	6/24/2008 7:17:32 PM	145	122A4B96	C2D9433A2AA9D7D53005704FF4F604A5
PDFXCVIEW.EXE-02F296AD.pf	6/20/2008 4:20:16 PM	6/20/2008 4:20:16 PM	6/20/2008 4:20:16 PM	6/20/2008 4:20:13 PM	1	2F296AD	340FCC150F47AD5B049B74F748B55E69
PGPMNAPP.EXE-2D29F457.pf	6/20/2008 4:58:26 PM	6/20/2008 4:58:26 PM	6/20/2008 4:58:26 PM	6/20/2008 4:58:23 PM	1	2D29F457	9F15C67DE56C777B9191C5AAA212DC7D
PIDGIN.EXE-1737386E.pf	6/19/2008 5:42:55 AM	6/23/2008 6:53:49 PM	6/19/2008 5:42:55 AM	6/23/2008 6:53:39 PM	5	1737386E	96DBD85DDB421ED594A1B0E28E9BE7EB

C:\Windows\Prefetch

A lot of discussions about prefetch lately.

Harlan Carvey has a great write up:
http://windowsir.blogspot.com/2007/05/prefetch-analysis.html

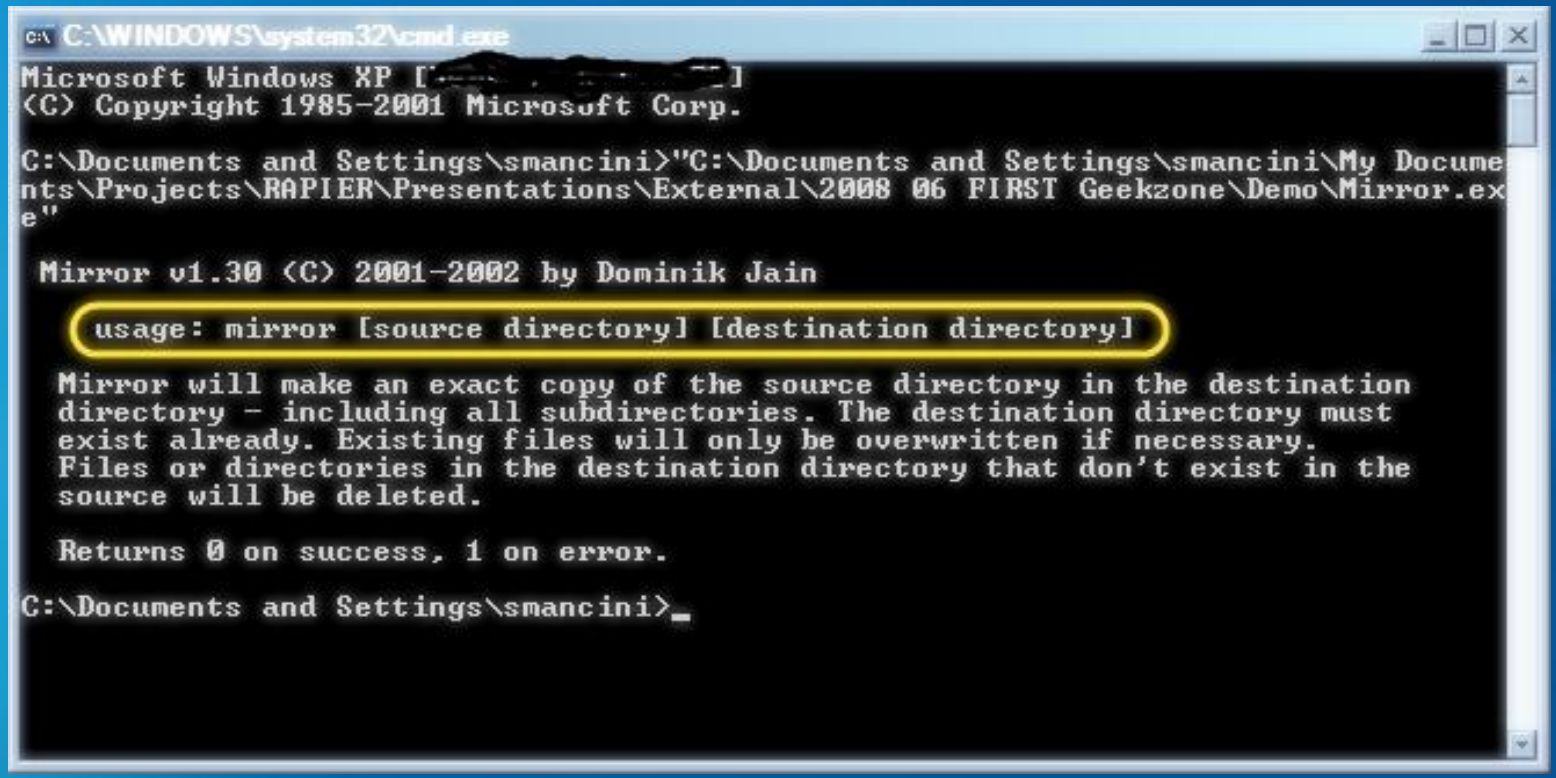
MiTec has created a tool called wfa (Windows File Analysis) that reports out about prefetch
http://www.mitec.cz/wfa.html

Dominik Jain has written a tool to mirror a directory.
http://home.in.tum.de/~jain/

We have everything we need…

First things first

Understand the output of the program:



Directory

- Easiest way is to copy another folder with like output and rework it.
- At minimum you want:
  - Module.cmd - the RAPIER wrapper
  - Module.wsf - the executable wrapper
  - Required_files.txt - what is needed
  - Your executable (in this case mirror.exe)

Edit Module.wsf

Define runtime constants:

```
'Define Constants
Const ModuleName="CmdLines"
Const Description="Determines the
  command line parameters associated
  with all running processes"
Const Author="Robbie Bytheway"
```

Cont'd

Define runtime constants:

```
'Define Constants
Const ModuleName="CopyPrefetch"
Const Description="Copies all files out
  of Prefetch directory"
Const Author="Steve Mancini"
```

Define Variables

```
'Define Variables
Dim StartTime, EndTime, ExecuteDuration,
  BitBucket,LogFile,Command
```

Startime, Endtime, Duration – used to calculate run time

BitBucket – all information written to the logfile

LogFile – defines were the logfile will reside

Command – the command to be executed

Cont'd

```
'Define Variables
Dim StartTime, EndTime, ExecuteDuration,
  BitBucket,LogFile,Command, Destination

Destination=CommandLineOptions() & "\" &
  ModuleName
```

We will need a destination directory – hence we add it and define it.

Change Command

Next you want to put the command line in the "Command=" section.

```
Command=CurrentWorkingDirectory() & "mirror.exe
  """ & SystemDrive() & "\Windows\Prefetch"" """
  LogDirectory & "\Prefetch"""

BitBucket=DirectoryMake(LogDirectory &
  "\PreFetch")

BitBucket=RunExternalApplication(Command)
```

Final Touches

Test (and re-test)

Roll into central distribution

Tell your incident handlers about the new module (and how to interpret)

(We'll be adding prefetch to the distro once we get permission to roll mirror.exe into the bundle)

RAPIER MODULE ANALYSIS

Forewarned…

You need to understand your (Microsoft's) image before you try to analyze what's going on:

- Systems to compare against = good
- File Integrity hashes = better
- System level integrity hashes = Superb

Feature Module Output

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

Module Output

System Configuration

Processes

Networking

Logs & Cache

Files

System Configuration

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

Questions to Ask…

System Configuration

- Examine the startup information – anything starting you do not know/understand?
- Examine the startup services – anything you do not understand?
  - http://www.blackviper.com/WinXP/servicecfg.htm
- Browse the patches installed – anything recent missing that would lead you to believe the system is not patched according to your org's policy?
- Is your anti-virus current?
- Drivers – yep they can be vulnerable, are yours loaded from known/expected paths? Current?
- Any local accounts you do not recognize?

Tools to Use…

System Configuration

- Content parsing – known good lists for your org's images are critical. Script a comparison tool vs output.
  - Run RAPIER on known good, compare
- MD5/SHA1 – just in case you find something interesting (default)
- PERL. Could be my unix background but it helps in parsing text files.
- Search Engines / Reputable Sites

Processes

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

Questions to Ask…

Processes

About the processes:

- What's running that you don't know about?
- Anything not known, but in the registry?
- No surprises in the execution paths?
- What ports are they tied to? Anything unexpected
- Anything interesting in the strings output of the memory-dumped processes?

And the DLL's (same deal)…

- How about in the paths to the loaded DLL's?
- Do the checksums match those on a known good system?

Anything installed that shouldn't be? (Kazaa, eMule)

Tools to Use…

Processes

- Strings.exe
- BitBlaze project (looks cool)
  - http://bitblaze.cs.berkley.edu
- IDA (if you are really hardcore)
- PE Tools, Unpackers
- MD5/SHA1 – submit it sites that track malicious code
- Mandiant Red Curtain
- iDefense Malware Analysis Pack

Networking

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- **Layer3 traffic samples**
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

58

Questions to Ask…

Networking

All the shares make sense?

Anything in promiscuous mode?

Virtual NICs? Should they be there?

Wireless vs. Wired?

Netstat – connections make sense? (You connected to machines you have no reason to be?)

Where is the traffic going?

How is it getting there? (routing tables, proxy)

What ports are listening - should they be?

Any unknown services bound to ports?

Tools to Use…

Networking

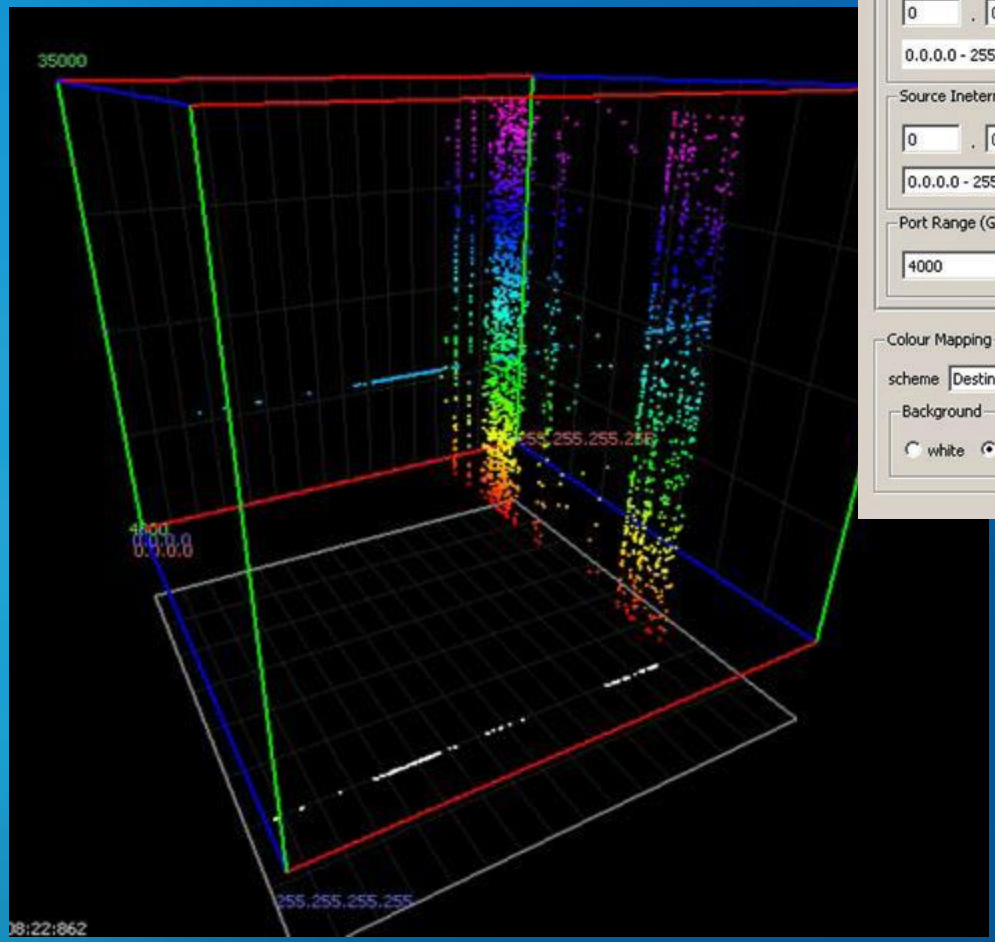
Strange outbound traffic

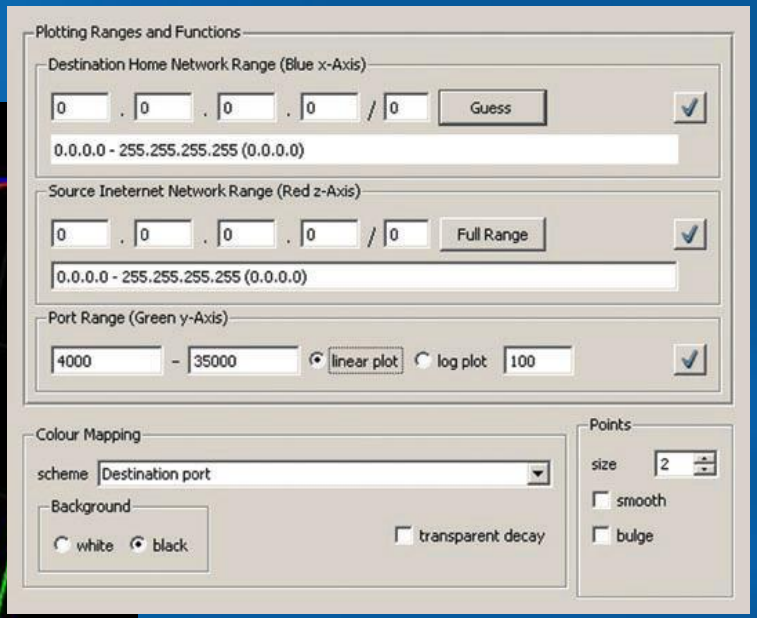
- Samspade.org – oldie but goodie
- Maltego (http://www.paterva.com/maltego/)
- Proxy server logs? (who else is connecting)

Good Traffic Capture/Analysis Tools:

- Tcpdump
- WireShark
- Rumit
- Time-Based Network Visualizer (tnv)
- Snort (replay mode rocks)
- NSM-Console (packet analysis)

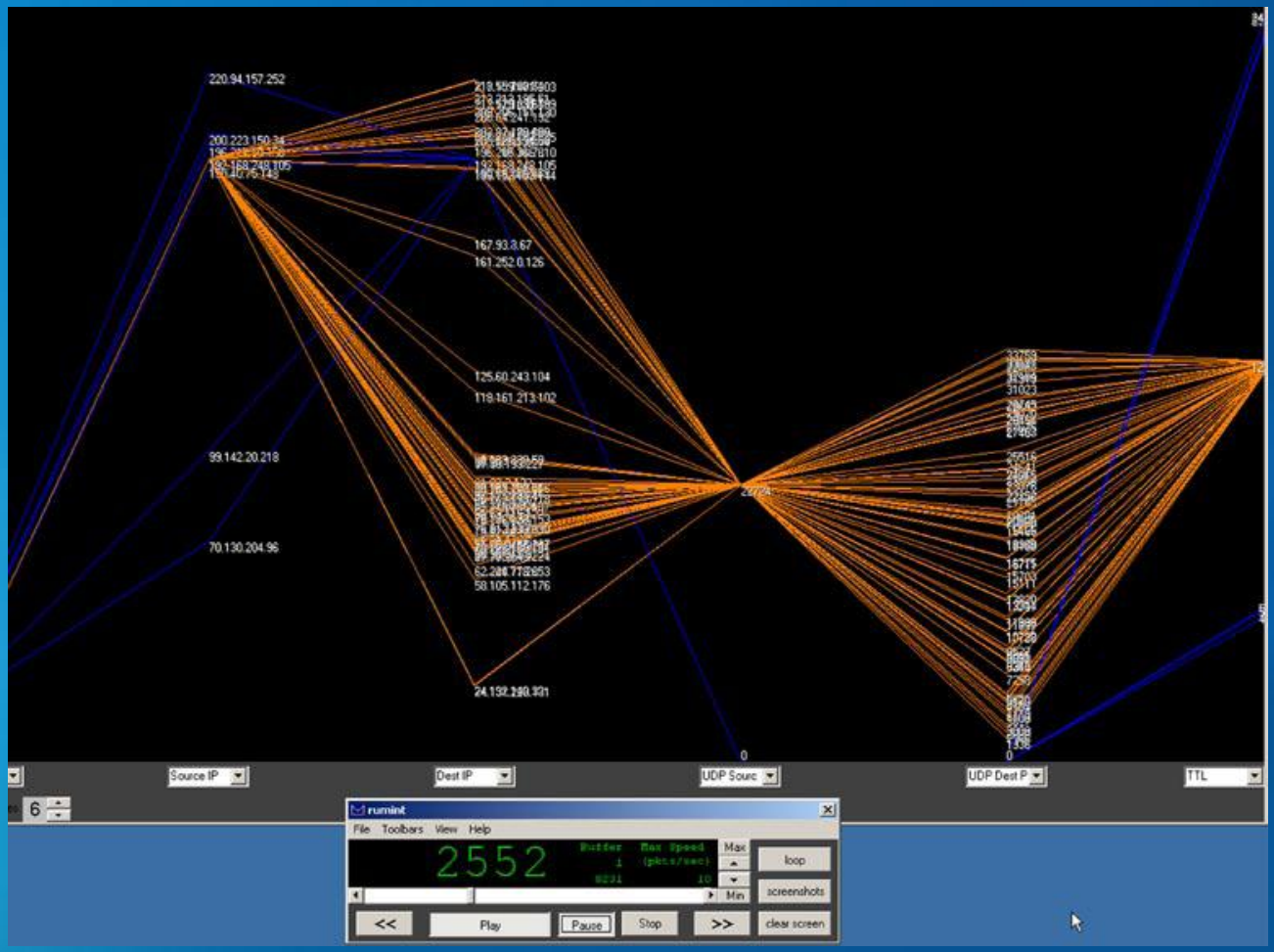
InetVis





A single Storm infection as visualized with InetVis

Rumint

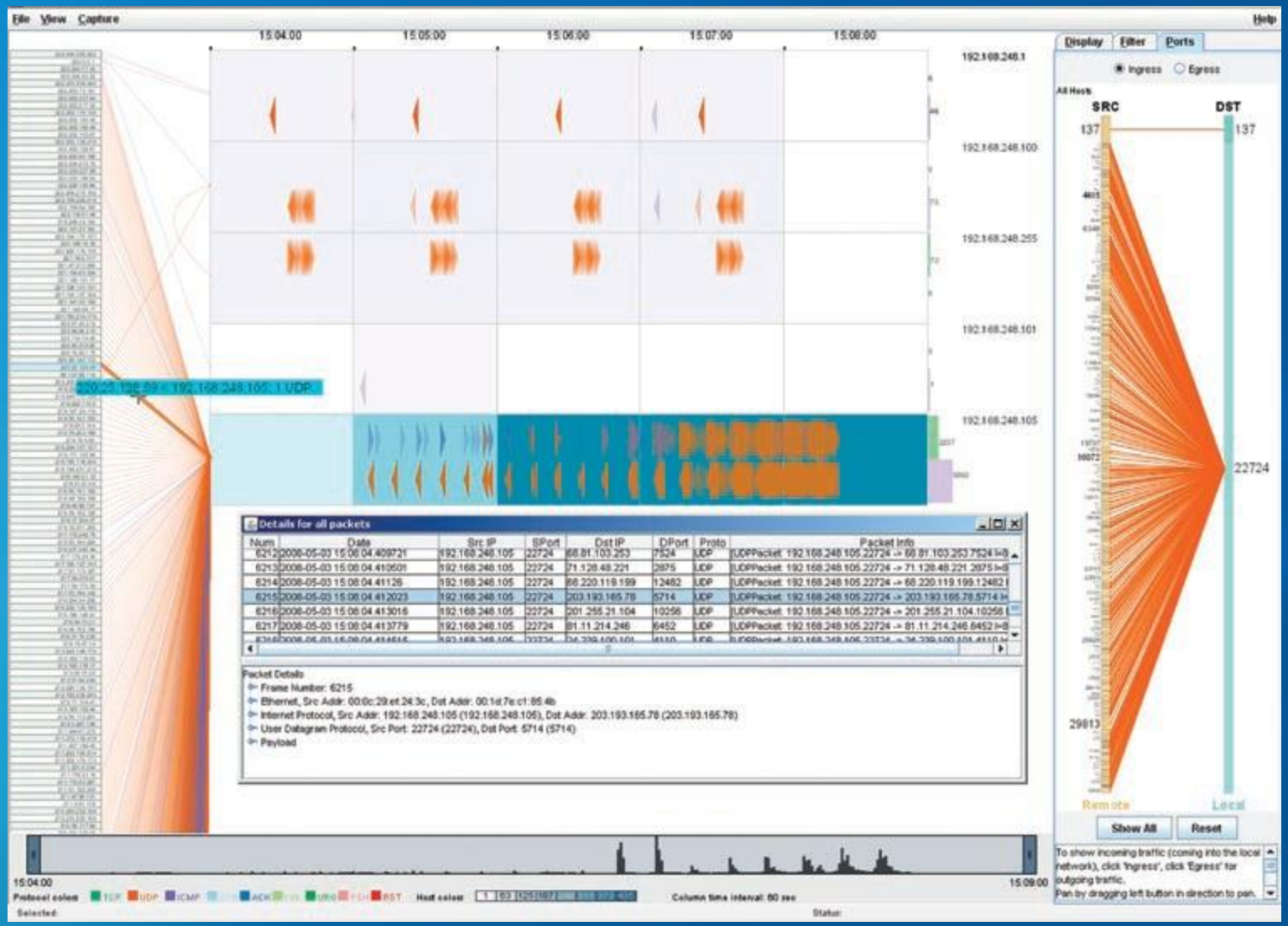


Visualized by
- Source IP,
- Dest IP,
- UDP Source,
- UDP Dest,
- TTL

using the same ecard.cap sample.

Greg Conti's excellent offering.

TNV



Notice all the connections from hundreds of IPs to a single infected host and egress to a single external destination port.

Logs & Cache

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

Questions to Ask…

Logs & Cache

- Are the logs start / last date what you might expect?
- Was AV running continuously until RAPIER was executed?
- Where did they go (websites) that were of interest? (examine output from cache)
- Deep dive on the content of the logs (how many does VISTA have? Ugh..)

Tools to Use…

Logs & Cache

Microsoft Log Parser (http://www.logparser.com)

Regviewer (unix) – tool to look at exported registry

Splunk – www.splunk.com (freeware version limited to 500MB per day)

Perl – (the unix guy in me again)

References:

http://windowsir.blogspot.com/2007/06/eventlog-analysis.html

http://www.logparser.com/

http://www.eventid.net

http://www.net-security.org/dl/insecure/INSECURE-Mag-16.pdf (Rob Faber)

Files

Volatile Information

- complete list of running processes
- locations of those processes on disk
- ports those processes are using
- Checksums for all running processes
- Dump memory for all running processes
- All DLLS currently loaded and their checksum
- Capture last Modify/Access/Create times for designated areas
- All files that are currently open
- Net (start/share/user/file/session)
- Output from nbtstat and netstat
- Document all open shares/exports on system
- Capture current routing tables
- list of all network connections
- Layer3 traffic samples
- capture logged in users

Static Information

- System Name
- Basic system info (peripherals, BIOS, drivers, etc)
- System Startup Commands
- MAC address
- List of installed services
- Local account and policy information
- Current patches installed on system
- Current AV versions
- Files with alternate data streams
- Discover files marked as hidden
- List of all installed software on system (known to registry)
- Capture system logs
- Capture of AV logs
- Copies of application caches (temporary internet files) – IE, FF, Opera
- Export entire registry
- Search/retrieve files based on search criteria.

Questions to Ask…

Files

- Any recently added or modifed that doesn't make sense?
- What is open? Why?
- Hidden files – should they be? (probably not)
- Alternate Data Streams?

Tools to Use…

Files

- Strings.exe
- MD5/SHA1 – submit it sites that track MD5's of malicious code
- Search Engines
- Jesse Kornblum's MissIdentify
- Mandiant Red Curtain
- iDefense Malware Analysis Pack

Over the horizon

- Sandman: Hibernation File examination
  - http://www.darknet.org.uk/2008/05/sandman-read-the-windows-hibernation-file/
- Change Analysis Diagnostic Tool (MSFT)
- Virtual Machine (discover/acquisition)
- Vista Logging
- Jesse Kornblum's MissIdentify (sourceforge.net)
- FCIV (file integrity prog from MSFT)
- SigVerif (MSFT) – verifies signed files
- MuiCache (application names/vers)
- Encrypt output (probably GPG)
- Par's cool stuff ☺

QUESTIONS, FEATURE REQUESTS & FEEDBACK

Your Thoughts/Questions

#include “conversation.h”

Website:

http://code.google.com/p/rapier/

Discussion:

http://groups.google.com/group/RAPIER-ramblings

Email:

Rapier.SecurityTool@gmail.com

Gratitude

Lawrence Baldwin (SecCheck*)
Jem Berkes (md5sums*)
Frank Heynes (LADS* tool)
Nir Sofer (cprocess*)
Arne Vidstrom (macmatch*, pmdump*)
Kevin Stanush (dumpsec*)
Parmavex Software (winaudit*)
Didier Stevens (BPMTK) – in development
Russ McRee (Evangelist and Contributor)
Harlan Carvey (his blog windowsir.blogspot.com keeps me busy.)

Jesse Kornblum for FRED* as a source of inspiration for most of the IR tools out there. (imho)

THANK YOU

To be continued at nearest bar…