MANDIANT

Jeff Hamm
hammjd@yahoo.com
jeff.hamm@mandiant.com
Senior Consultant

# Carve for Records
## Not Files

## Introduction Slide

MANDIANT

- Introductions
- Traditional File Carving Tools and Techniques
- Definitions
- Windows Event Logs
- Last Logs
- Web Logs
- Shell History Logs
- Historical IP Address
- Resources
- Q&A

## Important note

MANDIANT

**All information is derived from MANDIANT observations in non-classified environments**

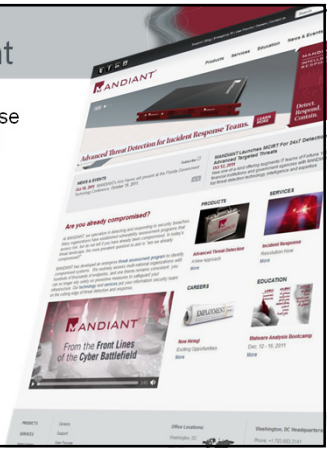
**Some information has been sanitized to protect our clients' interests**

## We are Mandiant

MANDIANT

- Threat detection, response and containment experts
- Software, professional & managed services, and education
- Application and network security evaluations
- Offices in
  - Washington
  - New York
  - Los Angeles
  - San Francisco



## Introductions

MANDIANT

**JEFF HAMM**

- Senior Consultant, MANDIANT
- Adjunct Lecturer, Gjøvik University College
- Former Sergeant, Oakland County Sheriff's Office, Michigan

## Traditional Data Carving Tools and Techniques

MANDIANT

**FULL FILE CARVING**

- Carving for Headers
- Option of Ending with a Footer
- Contiguous Clusters

**TOOLS**

- Full Suites
- One Trick Ponies
- Automated Processes
- Ability to Import Custom Headers



MANDIANT®

## Traditional File Carving Tools and Techniques

| EFFECTIVE | FILE TYPES |
|---|---|
| Digital Image Files | JPG |
| Video | AVI |
| Contiguous Clusters | RAR |

7 © Copyright 2012

## Traditional File Carving Tools and Techniques

| NOT AS EFFECTIVE | FILE TYPES |
|---|---|
| Event Logs | EVT(x) |
| Linux Last Logs | WTMP |
| Web Logs | LOG |
| Shell Histories | .history |
| Tracking Cookies | TXT or SQL |

8 © Copyright 2012

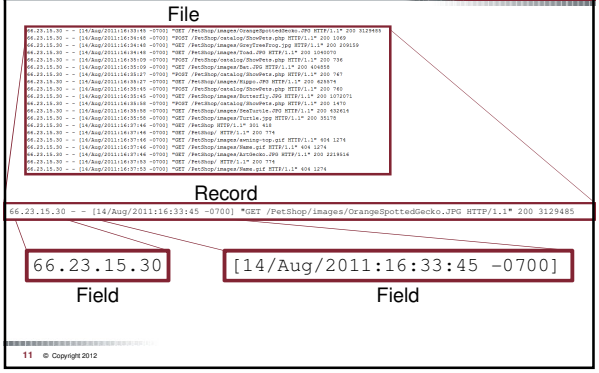
## Definitions

9 © Copyright 2012

## Definitions

10 © Copyright 2012

## Definitions




11 © Copyright 2012

## Definitions

| HOW TO SEARCH | LIMITATIONS |
|---|---|
| Need Knowledge of the Data Set/Type | 255 Characters |
| Regular Expressions | Commas in Data Fields |

12 © Copyright 2012

## Apache Log

Record

```
66.23.15.30 - - [14/Aug/2011:16:33:45 -0700] "GET /PetShop/images/OrangeSpottedGecko.JPG HTTP/1.1" 200 3129485
```

LogFormat

```
%h (IP Address)   %l (identd)   %u (user)   %t (date)   \"%r\" (request)   %>s (status)   %b (size)
```

Search by IP Address

```
grep "[1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?\.[1-9][0-9]?[0-9]?[\ \-]"
```

Search by Date

```
grep "{1?[0-9]\/Aug\/2011\:[0-9][0-9]\:[0-9][0-9][0-9][0-9]-]"
```

13 © Copyright 2012

## Apache Log Success

- BotNet Server
  - /var/log/apache
    - access_log
- Carving Results
  - Over 12 million
- Included Check-ins from compromised hosts

xx.xx.xxx.xxx - - [26/Jun/2010:18:17:05 -0400] "GET /spy/gate.php?guid=user1!HOST1!A889EB32&ver=10200&stat=ONLINE&cpu=0&ccrc=A1CC72AF&md5=1234a5217a92a88771b0a7982c1bb3d8 HTTP/1.1" 200 51
xxx.xxx.xxx.xx - - [26/Jun/2010:18:17:05 -0400] "GET /spy/gate.php?guid=user2!HOST2!B47CD21D&ver=10200&stat=ONLINE&cpu=1&ccrc=B2F96423&md5=56787689e35c396f16e4d035f56fb391 HTTP/1.1" 200 51

14 © Copyright 2012

## IIS Log

Record

```
04/19/12 23:32:12 xx.xx.xxx.x GET /owa/forms/premium/clientstrings.aspx v=14.2.283.3&l=en-US&Initial+Budget>>Conn:1,HangingConn:0,AD:18000/17985/1%,CAS:90000/89829/1%,AB:18000/18000/0%,RPC:90000/89864/1%,FC:1000/0,Policy:DefaultThrottlingPolicy_44275716-3554-4935-9720-bb162e562ebc,Norm&v=14.2.283.3&mbx=mail1.foo.company.int&sessionId=f6f3d8e11814a77b89bfd723d4f668a&prfltncy=2&prfrpccnt=0&prfrpclt ncy=0&prfldpcnt=0&prfldpltncy=0&prfavlcnt=0&prfavlltncy=0&End+Budget>>Conn:1,HangingConn:0,AD:18000/17985/1%,CAS:90000/89829/1%,AB:18000/18000/0%,RPC:90000/89864/1%,FC:1000/0,Policy:DefaultThrottlingPolicy_44275716-3554-4935-9720-bb162e562ebc,Norm 443 HelpDesk xxx.xx.xxx.xx Mozilla/5.0+(Windows+NT+6.1;+rv:5.0)+Gecko/20100101+Firefox/5.0 200 0 0 702
```

LogFormat

```
Date : Server IP : Method : URI Stem : URI Query : Source Port : User Name : Client IP : User Agent : Status : Substatus : Win32 Status : Time Taken
```

Expression

```
grep -a "2012-[0-9][0-9]-[0-9][0-9].[0-9][0-9]:[0-9][0-9][0-9][0-9][0-9] [0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\ [A-z]*\/.** Unallocated\ Clusters
```

15 © Copyright 2012

## IIS Log Success

- Exchange Server
  - C:\inetpub\logs\LogFiles\W3SVC1\u_ex120420.log
  - Logical Logs Only for April 2012
- Carving Results
  - 12,406,784 Recovered Web Log Records from Unallocated
  - January 3, 2012
    - Actually had entries back to July 22, 2011
- Included External Logins to OWA from Malicious IP Addresses
  - 3,000 Entries

16 © Copyright 2012

## Shell History Log

**BASH HISTORY**

- Plain text series of commands
- Only Identifier is EOL

**ZSHELL HISTORY**

- : 1338863410:0;ls
- : 1338863413:0;who
- : 1338863419:1;less mount_dd
- : 1338863423:0;exit

```
grep ":\ [0-9]\{10\}:[0-9];.*" .history
```

17 © Copyright 2012

## Shell History Log Success

```
mv /usr/bin/pkill /usr/bin/pkill.orig;cp /sysadm/hackers/pkill /usr/bin/pkill;mv /bin/kill /bin/kill.old;cp /sysadm/hackers/kill /bin/kill;mv /sbin/shutdown /sbin/shutdown.orig;cp /sysadm/hackers/shutdown /sbin/shutdown;mv /sbin/halt /sbin/halt.orig;cp /sysadm/hackers/halt;cp /sysadm/hackers/shutdown /sbin/shutdown;mv /sbin/halt /sbin/halt.orig;cp /sysadm/hackers/halt /sbin/halt
```

18 © Copyright 2012

## Shell History Log Success

| | |
|---|---|
| 02/25/2011 00:17:18 | mv /usr/bin/pkill /usr/bin/pkill.orig;cp /sysadm/hackers/pkill /usr/bin/pkill;mv /bin/kill /bin/kill.old;cp /sysadm/hackers/kill /bin/kill;mv /sbin/shutdown /sbin/shutdown.orig;cp /sysadm/hackers/shutdown /sbin/shutdown;mv /sbin/halt /sbin/halt.orig;cp /sysadm/hackers/halt /sbin/halt;cp /sysadm/hackers/shutdown /sbin/shutdown;mv /sbin/halt /sbin/halt.orig;cp /sysadm/hackers/halt /sbin/halt |
| 02/25/2011 00:17:48 | halt |
| 02/26/2011 17:54:02 | su – joeblow |
| 02/26/2011 23:11:44 | ls |
| 02/26/2011 23:11:50 | which pkill |
| 02/26/2011 23:12:14 | locate kill |
| 02/26/2011 23:12:17 | locate kill.orig |
| 02/26/2011 23:12:32 | mv /usr/bin/pkill.orig /usr/bin/pkill |
| 02/26/2011 23:12:37 | df |
| 02/26/2011 23:13:27 | ps -ef\|grep java |
| 02/26/2011 23:13:30 | which shutdown |
| 02/26/2011 23:13:34 | locate shutdown.orig |
| 02/26/2011 23:13:40 | mv /sbin/shutdown.orig /sbin/shutdown |
| 02/26/2011 23:13:47 | mv /sbin/halt.orig /sbin/halt |

## Last Log

**PARSERS**

- Coreutils
  - last –f <filename>
- Xways Template
- Only Deal with Files

**ADDITIONAL**

- -R Suppresses the display of the hostname field.
- -a Display the hostname in the last column. Useful in combination with the next flag.
- -d For non-local logins, Linux stores not only the host name of the remote host but its IP number as well. This option translates the IP number back into a hostname.
- -F Print full login and logout times and dates.
- -i This option is like -d in that it displays the IP number of the remote host, but it displays the IP number in numbers-and-dots notation.
- -o Read an old-type wtmp file (written by linux-libc5 applications).
- -x Display the system shutdown entries and run level changes.

## Last Log

**WTMP**

- l l a32 a4 a32 a256 s s l l l C C C C a32

| Type | PID | Device | Init | ID | User | Host | Process |
|---|---|---|---|---|---|---|---|
| Status | Exit | Status | Session | ID | Time | Microseconds | IP Address |

- White Space
- Grep for User Name

## Last Log

| Type | PID | Dev | Init ID | User | Host | Status | Exit | Session ID | Time | Time (Local) | Micro-seconds | IP Address |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 426 7 | pts/1 | ts/1 | thorsen | domain.user.com | 0 | 0 | 0 | 01/12/2011 22:08:40 | 01/12/2011 14:08:40 | 838968 | 10.20.2.10 |
| 8 | 426 7 | pts/1 | | | | 0 | 0 | 0 | 01/12/2011 22:09:44 | 01/12/2011 14:09:44 | 775107 | 0.0.0.0 |
| 7 | 127 11 | pts/1 | ts/1 | thorsen | 10.20.1.10 | 0 | 0 | 0 | 02/24/2011 00:51:29 | 02/23/2011 16:51:29 | 668240 | 10.20.2.10 |
| 8 | 127 11 | pts/1 | | | | 0 | 0 | 0 | 02/24/2011 00:52:26 | 2/23/2011 16:52:26 | 359088 | 0.0.0.0 |

## Last Log Success

- 78 Cent OS Servers
- Logical Volumes (lvm)
- On a 3 TB Logical Volume
- rm -fr /
- No Contiguous Files
- Two Actors
- Login Data After Termination
  - One from a public library

## Last Log Parsing Tool

- Perl
- Jeff Hamm: LinuxLast.pl
- Parses Entries
- Output in TSV or to Screen

## Windows Event Log

- Header
  - LfLe
- Entry Header
  - LfLe
- Length: Variable

## Windows Event Log

**EVT**

| Offset | Length | Field | Description |
|---|---|---|---|
| **Header** | | | |
| **0x00** | 4 bytes | Length | This is the length of the entire entry. |
| **0x04** | 4 bytes | Reserved | The "LfLe" signature. |
| **0x08** | 4 bytes | RecordNumber | The Event Record Number |
| **0x0C** | 4 bytes | TimeGenerated | Time the entry was submitted. |
| **0x10** | 4 bytes | TimeWritten | Time the entry was written to the log. |
| **0x14** | 4 bytes | EventID | Packed bytes – See Table 2. |
| **0x18** | 2 bytes | EventType | Event type (Error, Failure, Success, Information, or Warning) |
| **0x1A** | 2 bytes | NumStrings | The number of strings in the log entry description. |
| **0x1C** | 2 bytes | EventCategory | Category of the event specific to the source. |
| **0x1E** | 2 bytes | ReservedFlags | Reserved. |
| **0x20** | 4 bytes | ClosingRecordNumber | Reserved. |
| **0x24** | 4 bytes | StringOffset | (L1) Offset to the description of the log entry. |
| **0x28** | 4 bytes | UserSidLength | (S2) The size of the UserSID (zero if no user identifier). |
| **0x2C** | 4 bytes | UserSidOffset | (L2) Offset to the UserSID. |
| **0x30** | 4 bytes | DataLength | (S3) Size of the event specific data. |
| **0x34** | 4 bytes | DataOffset | (L3) Offset to the event specific data. |
| **Data** | | | |
| | Variable String | SourceName | |
| | Variable String | Computername | |
| **L2** | S2 | UserSid | |
| **L1** | Variable String | Strings | Pad with zeros to end the entry on a DWORD boundary |
| **L3** | S3 | Data | |
| | CHAR | Pad | Pad with zeros to end the entry on a DWORD boundary |
| | 4 bytes | Length | The length of the entire entry |

## Windows Event Log

grep "LfLe"

## Windows Event Log Success

- Logs Cleared
- Pagefile.sys
- Retrieved Over 200,000 Records
- PsExec.exe Started
- PsExec.exe Stopped
- Compromised Account Logins

## Windows Event Log Tool

- Python
- Willi Ballenthin: lfle.py
- Searches any data set
- Parse with log2timeline with "-f" switch
  - version 0.51 only

## Historical IP Address

**REGISTRY AND SETTINGS**

- Windows and Linux Record DHCP/NAT Address Locally
- Router Logs Assignments
- Typical Home Setup Won't Log Historical Data

**COOKIE FILES**

- WebTrend First Person Cookies (WTFPC)
- Twitter "k" Cookie
- Part of User ID is External IP

## Historical IP Address

**WT_FPC**

- GUID and Time Stamp
  - GUID Often Contains an IP
  - Time Stamp in UNIX

```
([a-zA-Z0-9]+)?\.[a-zA-Z0-
9]+\.[a-zA-Z0-
9]+WT\_FPCid\=[1-2]?##?\.[1-
2]?##?\.[1-2]?##?\.[1-
2]?##?.{0,100}lv\=#######{0,
7}(\:ss\=#######{0,7}){0,1}
```

- document.cookie="WT_FPC=id=*VisitorID*:lv=*Timestamp*:ss=*Timestamp*; expires=*Date*; path=/; domain=*CookieDomainAttribute*";

**TWITTER "K"**

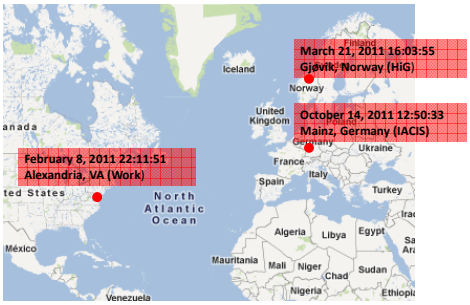
- GUID and Time Stamp
  - GUID Contains an IP
  - Time Stamp in UNIX

```
([a-zA-Z]+)?\.[a-zA-
Z]+\.[a-zA-Z]+[1-
2]?##?\.[1-
2]?##?\.[1-
2]?##?\.[1-
2]?##?.#######{0,10}
```

- domain;cookie name;ip address;last visit date

## Historical IP Address



## Historical IP Address

| Visit Count | Site | Cookie Name | IP Address | Date | Geolocation |
|---|---|---|---|---|---|
| 4 | .twitter.com | K | xx.xx.xx.xx | 02/08/2011 22:11:51 | Alexandria, VA |
| 5 | www.xe.com | ID | xx.xx.xx.xx | 03/21/2011 16:03:55 | Norway |
| 4 | www.rollcall.com | Apache | xx.xx.xx.xx | 06/01/2011 15:12:52 | Alexandria, VA |
| 1 | .twitter.com | k | xx.xx.xx.xx | 06/01/2011 16:48:43 | Alexandria, VA |
| 2 | .twitter.com | k | xx.xx.xx.xx | 07/05/2011 12:00:12 | Alexandria, VA |
| 12 | .twitter.com | k | xx.xx.xx.xx | 08/14/2011 20:44:40 | Home |
| 1 | .twitter.com | k | xx.xx.xx.xx | 08/19/2011 12:46:27 | Alexandria, VA |
| 2 | .twitter.com | k | xx.xx.xx.xx | 09/01/2011 13:38:16 | Alexandria, VA |
| 2 | .twitter.com | k | xx.xx.xx.xx | 09/16/2011 18:10:32 | Alexandria, VA |
| 7 | .unica.com | UnicaID | xx.xx.xx.xx | 09/28/2011 17:26:59 | Verizon Wireless |
| 4 | www.networld.com | Apache | xx.xx.xx.xx | 09/30/2011 15:27:29 | Alexandria, VA |
| 5 | .splunk.com | Apache | xx.xx.xx.xx | 10/14/2011 12:50:33 | Germany |
| 6 | wstat.wibiya.com | Apache | xx.xx.xx.xx | 11/15/2011 17:33:19 | Norway |
| 4 | www.dividendmilesstorefront.com | Apache | xx.xx.xx.xx | 11/23/2011 12:49:21 | Alexandria, VA |

## Historical IP Address Success

- Suspect's Machine
- Unauthorized Access to Remote Servers
- Denial of Service Floods
- Remote Administration of BotNet Servers
- Reinstalled the Operating System Prior to Seizure
- Recovered Historical IP Data
  - 6 months worth

## Additional Thoughts

- SQL
- Index.dat
- Virtually Any Known Record Format
- "Deleted" Registry Keys
- Don't Forget:
  - Pagefile
  - Memory Images
- The Records Are the Key, Not the File
- If You Can Parse the Data, You Can Carve it
- Limited by Expression Size
- More Data Means More Trimming
- Compression?
- Encryption?

## Free resources

- Free tools
  - IOCe
  - Memoryze
  - Audit Viewer
  - Highlighter
  - Red Curtain
  - Web Historian
  - First Response
- Resources
  - M-trends
  - M-unition
    - blog.mandiant.com
- Education
  - Black Hat classes
  - Custom classes
- Webinar series
  - Sign up

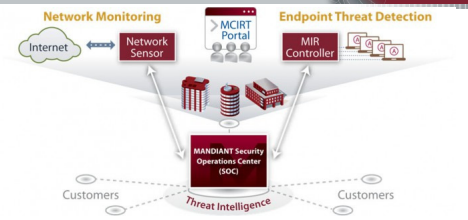
 

## Intelligent Response

- Find indicators of compromise on thousands of hosts
- Live IR on thousands of systems at once
- From disk images to registry keys to live memory forensics
- It's part of almost every response we do

## MCIRT




- 24 x 7 monitoring by Mandiant's team of expert threat analysts
- Sweeps all endpoints to identify advanced targeted attacks
- Inspect network traffic to identify ongoing targeted attacks
- Correlates indicators of attack against the most recent tactics

## Q&A



## MANDIANT is hiring

*Alexandria, VA*
*Reston, VA*
*New York, NY*
*Los Angeles, CA*
*Redwood City, CA*
*San Francisco, CA*
*Dallas, TX*
*Chicago, IL*
*Seattle, WA*

- Positions in
  - Product development
  - Consulting, federal and managed services
  - Sales
  - Marketing
- http://www.mandiant.com/hireme

MANDIANT

**Jeff Hamm**
**hammjd@yahoo.com**
**jeff.hamm@mandiant.com**
Senior Consultant

## Carve for Records
**Not Files**



MANDIANT®