

LIVE DATA COLLECTION

INTRODUCTION

- Live data is collected in nearly every incident response investigation
- The main purpose of the collection is to preserve volatile evidence that will further the investigation.
- It is done to begin answering investigative questions without performing a more lengthy drive duplication.
- It helps you get answers quickly so you can reduce the risk of data loss or other negative consequences of an incident.
- The result should also help decide if a full drive duplication is necessary

INTRODUCTION

- It comes with a risk
- Important consideration is to minimize changes to the system made due to the collection process
- Automated processes are used to prevent excessive and unnecessary changes to the system

WHEN TO PERFORM A LIVE RESPONSE

- There are five important factors to consider when deciding if a live response is appropriate in your current situation
 - Is there a reason to believe volatile data contains information critical to the investigation that is not present elsewhere?
 - Can the live response be run in an ideal manner, minimizing changes to the target system?
 - Is the number of affected systems large, making it infeasible to perform forensic duplications on all of them?

WHEN TO PERFORM A LIVE RESPONSE

- There are five important factors to consider when deciding if a live response is appropriate in your current situation
 - Is there risk that forensic duplications will take an excessive amount of time, or potentially fail?
 - Are there legal or other considerations that make it wise to preserve as much data as possible?

WHEN TO PERFORM A LIVE RESPONSE

- Always evaluate the following questions to determine if the risk of performing the live response is too great to neglect:
 - Have you tested the live response process on a similar system?
 - Is the system particularly sensitive to performance issues?
 - If the system crashes, what would the impact be?
 - Have you communicated with all stakeholders and received their approval? In some cases, written approvals may prudent.

SELECTING A LIVE RESPONSE TOOL

- There are few consideration to evaluate which solution to go for:
 - Is the tool generally accepted in the forensic community?
 - Does the solution address the common operating systems in environment?
 - Does the solution collect data that is important to have, based on your environment?
 - How long does a collection take?
 - Is the collection configurable?
 - Is the output easily reviewed and understood?

IS THE TOOL GENERALLY ACCEPTED IN THE FORENSIC COMMUNITY?

- There are certain requirements for admissibility of evidence in the court.
- The tools and procedures you use throughout an investigation should meet these requirements.
- Acceptability involves considerations in many areas, including logging, chain of custody, cryptographic checksums and sound procedures and algorithms
- If the tools you decide to use are not generally recognized and accepted in the forensic community for the purposes you are using them for, you will increase the risk that your results will be disputed.

DOES THE SOLUTION ADDRESS THE COMMON OPERATING SYSTEMS IN YOUR ENVIRONMENT?

- Microsoft Windows might be one of the more popular operating systems.
- But many environments have a mixture of Windows, Unix, Apple, and others. What happens when one of those systems is compromised?
- You should have live response tools that address all of the common operating systems that are used in your environment.

DOES THE SOLUTION COLLECT DATA THAT IS IMPORTANT TO HAVE, BASED ON YOUR ENVIRONMENT?

- Understanding what data is important will help you choose a proper solution for your organization.
- You should collect data that is the most likely to help answer common questions and provide leads. Part of what you collect should be based on the software and configuration of the systems in your environment.
- For example, it may be useful to collect log files from security or other software programs.

HOW LONG DOES A COLLECTION TAKE?

- A goal of performing a live response is to get answers quickly.
- Therefore, the live response collection should not take a long time to complete.

IS THE COLLECTION CONFIGURABLE?

- In some environments, we find that collecting certain pieces of information are problematic.
- In other cases, we need to collect additional data that is not part of a standard live response process.
- It's important for the collection tool to be configurable, so you can add or remove items to collect.

IS THE OUTPUT EASILY REVIEWED AND UNDERSTOOD?

- A GUI interface is nice but The access to the raw data is preferred as it would allow investigator to perform custom analysis using scripts or other tools.
- Structured data is much more acceptable because there are many tools to deal with viewing, sorting and filtering those formats such as CSV, XML, TSV.

WHAT TO COLLECT

- In most cases, investigative team collect from two general categories, :
 - Data that describes the current running state of the system such as network connections and running processes. This data, typically contents system memory, provides information that helps to answer questions about what is happening now.
 - The second category is information that is less volatile and provides a snapshot of important information that can answer questions about what happened in the past – for example, a file listing, system logs or other operating system or application specific data.

WHAT TO COLLECT

- At a minimum, the live response tool you choose should be capable of collecting the following common live response data from a system:
 - The system time and date, including the time zone
 - Operating system version information
 - General system information, such as memory capacity, hard drives, and mounted file systems
 - List of services and programs configured to automatically start on boot-up, such as web servers, databases, multimedia applications, and e-mail programs
 - List of tasks scheduled to automatically run at given times or intervals
 - List of local user accounts and group membership

WHAT TO COLLECT

- At a minimum, the live response tool you choose should be capable of collecting the following common live response data from a system:
 - Network interface details, including IP and MAC addresses
 - Routing table, ARP table, and DNS cache
 - Network connections, including associated processes
 - Currently loaded drivers or modules
 - Files and other open handles
 - Running processes, including details such as parent process ID (PID) and runtime

WHAT TO COLLECT

- At a minimum, the live response tool you choose should be capable of collecting the following common live response data from a system:
 - System configuration data
 - User login history, including user name, source, and duration
 - Standard system log data
 - List of installed software
 - Appropriate application log data—web browser history, antivirus logs, and so on
 - Full file system listing, including the appropriate timestamps for the file system

COLLECTION BEST PRACTICES

- There are few considerations that can help an investigator establish a good process:
 - Document exactly what you do and when you do it. You'll need to note the difference between the actual time and system time. Don't forget to include time zone in your notes.
 - Treat the suspect computer as “hot”—do not interact with it unless you have a plan. Get on and off the system as quickly as possible.
 - Use tools that minimize the impact on the target system. Avoid GUI-based collection tools; instead, use tools that have a minimal memory profile and that do not make unnecessary or excessive changes to the target system.

COLLECTION BEST PRACTICES

- There are few considerations that can help an investigator establish a good process:
 - Use tools that keep a log and compute cryptographic checksums of their output as the output is created (not after the fact).
 - Fully automate the collection process, perhaps eliminating the requirement for a human to interact with the suspect computer.
 - Do your best to collect data in order of volatility.

COLLECTION BEST PRACTICES

- There are few considerations that can help an investigator establish a good process:
 - Treat the data you collect as evidence—be sure to follow your data preservation procedures, including the creation of an evidence tag and chain of custody. Don't forget to compute an MD5 checksum of the evidence.
 - Consider files on media you connect to the suspect computer as lost to the attacker. For example, do not keep indicators, documents, reports, notes, or anything else on the media from which the live response will be run.
 - Consider any credentials you use as compromised. It's a good idea to use an account other than your primary account, and change the password frequently or use a two-factor or one-time password solution.

COLLECTION BEST PRACTICES

- There are few considerations that can help an investigator establish a good process:
 - Do not take actions that will cause unnecessary modifications to the suspect computer unless there is no other option, such as copying the live response kit to the system or storing the output there. Doing so may destroy valuable evidence. Use removable media, a network share, or other remote media options.
 - Do not use the suspect computer to perform analysis. This causes unnecessary changes to the system, potentially destroying evidence and making it harder to discern attacker activity from responder activity. You also do not know what state the system is in—it could be providing incorrect results.

LIVE DATA COLLECTION ON WINDOWS SYSTEM

Windows Built-in Tools

Copy these files from a clean Windows system

Also copy cmd.exe

"Trusted binaries"

Don't trust files on the evidence machine

Data Collected	Command(s)
System date and time	date and time
Time zone	systeminfo
Installed software	
General system information	
OS version	
Uptime	
File system information	
User accounts	net user
Groups	net group
Network interfaces	ipconfig/all
Routing table	route print
ARP table	arp -a
DNS cache	ipconfig/displaydns
Network connections	netstat -abn

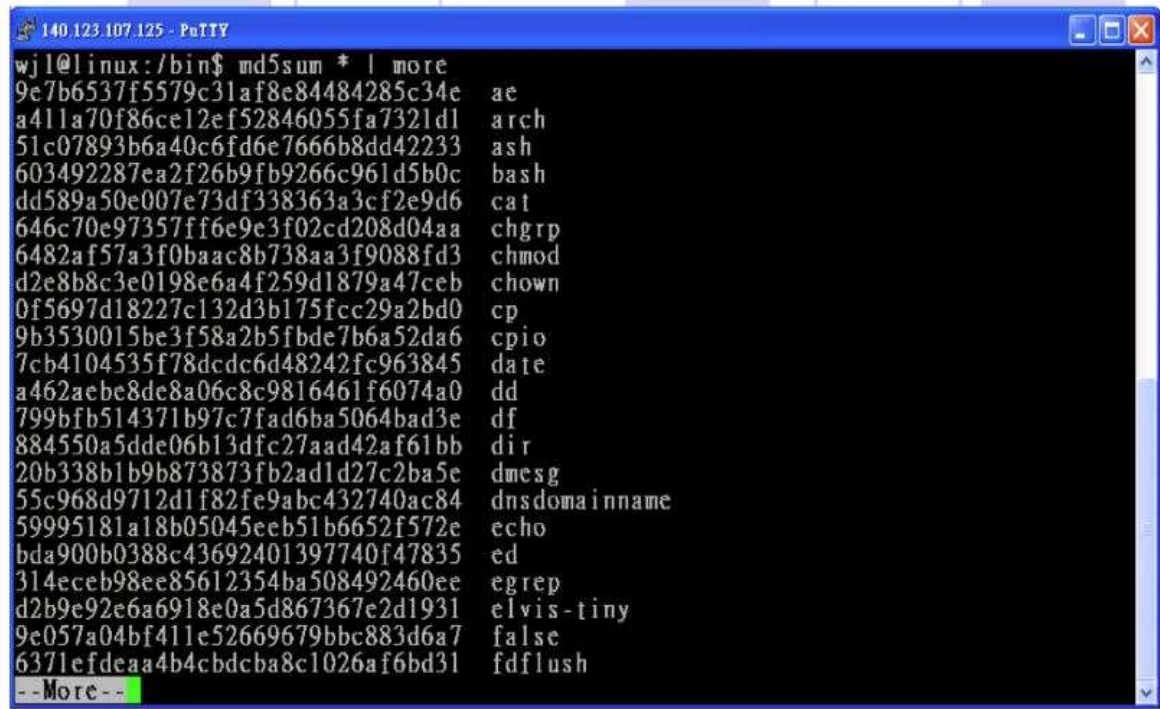
LIVE DATA COLLECTION ON WINDOWS SYSTEM

cmd.exe	The command prompt for Windows NT/2000/XP	Built in
PsLoggedOn	A utility that shows all users connected locally and remotely	www.foundstone.com
rasusers	Show which users have remote-access privilege on the target system	NT Resource Kit (NTRK)
netstat	Enumerate all listening ports and all current connections to those ports	Built in
Fport	Enumerate all processes that opened any TCP/IP ports on a windows NT/2000/XP	www.foundstone.com
Pslist	Enumerate all running processes on the target system	www.foundstone.com
ListDLLs	List all running processes (command-line argument, DLLs)	www.foundstone.com
nbstat	List the recent NetBIOS connections for approximately the last 10 mins	Built in
arp	Show the MAC addresses of the systems that the target system has been communicating	Built in
kill	Terminate a process	NTRK

LIVE DATA COLLECTION ON WINDOWS SYSTEM

md5sum	Create MD5 hashes for a given file	www.cygwin.com
rmtshare	Display the shares accessible on a remote machine	NTRK
netcat	Create a communication channel between two different systems	www.atstake.com/research/tools/network_utilities
cryptcat	Create an encrypted channel of communication	http://Sourceforge.net/projects/cryptcat
PsLogList	Dump the contents of the event logs	www.foundstone.com
ipconfig	Display interface configuration information	Built in
PsInfo	Collect information about the local system built	www.foundstone.com
PsFile	Show files that are opened remotely	www.foundstone.com
PsService	Show information about current processes and threads	www.foundstone.com
auditpol	Display the current security audit settings	NTRK
doskey	Display the command history for an open cmd.exe shell	Built in

LIVE DATA COLLECTION ON WINDOWS SYSTEM



```
140.123.107.125 - PuTTY
wjl@linux:/bin$ md5sum * | more
9e7b6537f5579c31af8e84484285c34e  ae
a411a70f86ce12ef52846055fa7321d1  arch
51c07893b6a40c6fd6e7666b8dd42233  ash
603492287ea2f26b9fb9266c961d5b0c  bash
dd589a50e007e73df338363a3cf2e9d6  cat
646c70e97357ff6e9e3f02cd208d04aa  chgrp
6482af57a3f0baac8b738aa3f9088fd3  chmod
d2e8b8c3e0198e6a4f259d1879a47ceb  chown
0f5697d18227c132d3b175fcc29a2bd0  cp
9b3530015be3f58a2b5fbde7b6a52da6  cpio
7cb4104535f78dc6d48242fc963845  date
a462aeb8e8de8a06c8c9816461f6074a0  dd
799bfb514371b97c7fad6ba5064bad3e  df
884550a5dde06b13dfc27aad42af61bb  dir
20b338b1b9b873873fb2ad1d27c2ba5e  dmesg
55c968d9712d1f82fe9abc432740ac84  dnsdomainname
59995181a18b05045eeb51b6652f572e  echo
bda900b0388c43692401397740f47835  ed
314eceb98ee85612354ba508492460ee  egrep
d2b9c92e6a6918e0a5d867367e2d1931  elvis-tiny
9e057a04bf411e52669679bbc883d6a7  false
6371efdeaa4b4cbdcba8c1026af6bd31  fdflush
--More--
```

LIVE DATA COLLECTION ON WINDOWS SYSTEM

Free Tools

- **Use command-line versions, not GUI versions**
 - **Easier to script**
 - **Less impact**
- **Rename every tool so you can identify it as something you added to the system**
- **Prepend "t_"**

Data Collected	Tool Name
Network connections	DiamondCS openports (www.softpedia.com)
List of services and tasks	Microsoft autoruns
Loaded drivers	NirSoft DriverView
Open files and handles	NirSoft OpenedFilesView
Running processes	Microsoft pslist
Registry (config data)	Microsoft logparser
Event logs (login history)	Microsoft logparser
File system listing	Microsoft logparser
LR output checksum computation	PC-Tools.net md5sums or hashutils (code.kluu.org/misc/hashutils)

Memory Collection

- **Tools for a full memory dump**
 - **AccessData FTK Imager Lite**
 - **Mandiant Memoryze**
 - **Monsools Windows Memory Toolkit**
 - **Belkasoft RAM Capturer**

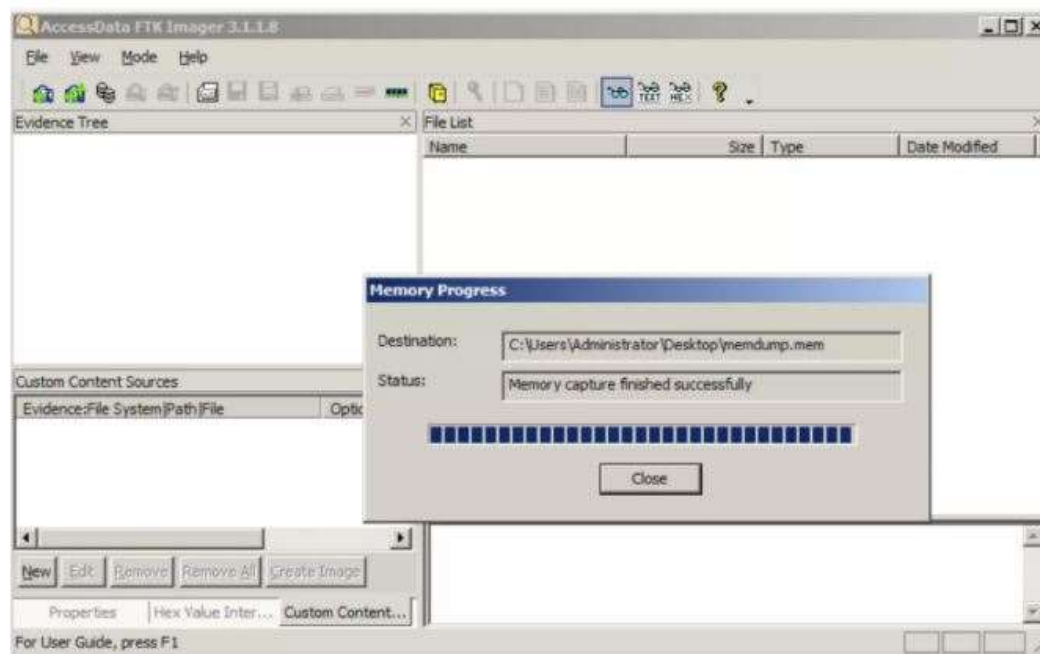
Mandiant Memoryze

- **Command-line tool: MemoryDD.bat**

```
<snip>
Beginning local audit.
Audit started 05-08-2012 20:21:23
Checking if 'D:\Downloads\LR\Memoryze\Audits\JASON-PC\2012050900
2123' exists...
Saving batch result to 'D:\Downloads\LR\Memoryze\Audits\JASON-PC
\20120509002123\'.
Batch results written to
'D:\Downloads\LR\Memoryze\Audits\JASON-PC\20120509002123\'.
Auditing (w32memory-acquisition) started 05-08-2012 20:21:23
Executing command for internal module w32memory-acquisition, 1.3.22.2
<Issue number="0" level="Info" summary="System range 0x0000000000000000 -
0x00000000000009d000" context="EnumerateDevices"/>

<Issue number="7022" level="Warning" summary=
"Unable to read memory page(s)Invalid address range 0x00000000bf780000 -
0x00000000ffff000" context="MapPhysicalMemory"/>
```

AccessData FTK Imager Lite



LIVE DATA COLLECTION ON UNIX SYSTEM

Built-in Unix Tools

Data Collected	Tool Name	License
System date and time	The date command	Part of operating system
Installed software	Debian-based: The dpkg --get-selections command RPM-based: The rpm -qa command BSD-based: The pkg_info command OS X: Copy the file /Library/Receipts/InstallHistory.plist	
File system information	The mount, df, and fdisk -l commands	Part of operating system
OS version	The cat /etc/issue command (Varies with operating system)	Part of operating system
Kernel version	The uname -a command	Part of operating system
Uptime	The w command	Part of operating system
Cron	Create a tar of cron files, normally kept in /var/spool/cron	Part of operating system

LIVE DATA COLLECTION ON UNIX SYSTEM

Built-in Unix Tools

Data Collected	Tool Name	License
Services	Varies by init system	Part of operating system
User accounts	The cat /etc/password and cat /etc/shadow commands	Part of operating system
Groups	The cat /etc/group command	Part of operating system
Network interfaces	The ifconfig -a command	Part of operating system
Routing table	The netstat -rn command	Part of operating system
ARP table	The arp -a command	Part of operating system
Network connections	The netstat -anp command	Part of operating system
Loaded drivers	Linux: The lsmod command BSD: The kldstat command OS X: The kextstat command (Varies for other operating systems)	Part of operating system

LIVE DATA COLLECTION ON UNIX SYSTEM

Built-in Unix Tools

Open files and handles	The lsof command	Free, commonly installed
Running processes and threads	Linux: The ps auxwwwem command (Varies for other operating systems)	Part of operating system
Configuration data (copy of files)	Create a tar of /etc (for example, tar cvfz /path/to/media/host-etc.tar.gz /etc/)	Part of operating system
System logs (copy of files)	Normally in /var/log or /var/adm or /Private/var/log (OS X), but varies between operating systems	Part of operating system
User shell history (copy of files)	BASH: .bash_history SH: .history (Varies with shell)	Part of operating system
File system listing	The find / -xdev -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s%p\n" command, or if find is not installed: The ls -alRu / command (atime) The ls -alRc / command (ctime) The ls -alR / command (mtime)	Part of operating system
LR output checksum computation	The md5 or md5sum command	Normally part of operating system

LIVE DATA COLLECTION ON UNIX SYSTEM

Memory Collection

- **The memory device is handled differently in every version of Unix, BSD, and Linux**
- **In earlier versions, you could just use dd to collect RAM through the /dev/mem device**
- **Direct access to memory os now blocked for security reasons**
- **Use LiME – Linux Memory Extractor ([link Ch 7c](#))**

LIVE DATA COLLECTION ON ANDROID/MAC SYSTEM

Collection from Apple OS X

- **Memoryze for Mac (link Ch 7d)**
 - **Mac Memory Reader seems to be gone**

```
system1:memoryze4mac root# ./macmemoryze dump -f system1_memory.dd
INFO: loading driver...
INFO: opening /dev/mem...

INFO: dumping memory to [system1_memory.dd]
INFO: dumping 5637144576-bytes [5376-MB]
INFO: dumping [5637144576-bytes:5376-MB] 100%
INFO: dumping complete
INFO: unloading driver...
system1:memoryze4mac root#
```

LIVE DATA COLLECTION ON ANDROID/MAC SYSTEM

Individual Process Dump

- **"gcore" (part of gdb, the GNU debugger)**

```
gcore -o /mnt/usb/case12-tag001-pid4327-sysauthd.img 4327
```

LIVE DATA COLLECTION ON ANDROID/MAC SYSTEM

- **system_profiler**
- **Very long list of software, hardware, logs, etc.**

Applications:

Microsoft Word:

```
Version: 15.20
Obtained from: Identified Developer
Last Modified: 3/19/16, 9:38 AM
Kind: Intel
64-Bit (Intel): No
Signed by: Developer ID Application: Microsoft Corporation (UBF8T346G9), Developer ID Certification Authority
Location: /Applications/Microsoft Word.app
Get Info String: 15.20 (160315), © 2016 Microsoft Corporation. All rights reserved.
```

LIVE DATA COLLECTION ON ANDROID/MAC SYSTEM

system_profiler

Media Player – Windows XP Professional:

```
Version: VMware Fusion 8.0.2
Obtained from: Identified Developer
Last Modified: 3/22/16, 7:55 PM
Kind: Intel
64-Bit (Intel): Yes
Signed by: Developer ID Application: VMware, Inc. (Fusion) (8J7TAMPT4P), Developer ID Certification Authority
Location: /Users/sambowne/Downloads/CCTF/Win2/XP_Machine/Applications/Media Player – Windows XP Professional
Get Info String: Windows XP Professional
c:/windows/system32/mplay32.exe
```

Camera:

FaceTime HD Camera:

```
Model ID: Apple Camera VendorID_0x106B ProductID_0x1570
Unique ID: DJH54345LFCG1HPBA
```