

Basic Incident Response and Computer Forensics

Kevin Thompson, CISSP
Information Security Manager
Minnesota State University, Mankato

&

Christophe Veltsos, CISSP, CISA, GCFA
Assistant Professor
Minnesota State University, Mankato

About this presentation

- How do you respond to an information security breach?
- What policies do you need to have in place ahead of time?
- Who needs to be notified within your organization?
- When do you notify your customers or employees?
- How do you know when to contact law enforcement and who should I call?
- How do you safely collect evidence in case you decide to contact law enforcement later?

Lecture Outline

- Preparing for Incident Response
 - Developing an Incident Response Plan
 - Making contact with law enforcement entities
 - Post Incident Review
- How to respond during an incident
 - Live system acquisition
 - Dead system acquisition
 - Maintaining Chain of custody

Developing an Incident Response plan

- Just because IR is reactive, doesn't mean you can't be proactive!
- This is the **MOST IMPORTANT** step in responding to an incident, being prepared for the response.
- It's not a question of IF, it's a question of **WHEN**
- “Immature strategy is the cause of grief”
 - Miyamoto Musashi (1584-1645)

Who's in charge here?

- In any crisis situation, the first thing you'll want to do is get everyone moving in the same direction.
- So your Incident Response Plan (IRP) should specify who is going to be in charge when an incident arises. This person is responsible for executing the IRP or delegating authority.

Who's in charge here

- It is very convenient to have a single point of contact for law enforcement and other people in the organization to talk to.
- Don't wait for someone to step forward and coordinate the troops, designate a leader ahead of time.
- Get that person some training in Incident Response.

How do users report an incident?

- Most of the time you'll find out about an information security incident because a user will bring it to your attention.
- Your IRP should provide instructions to the users on who to contact when they think something is amiss.
 - That brings me to Subtopic 1

Subtopic 1 – User Education

- Users can't report security incidents if they don't know what a security incident is.
- You should strongly consider having a training program in place to teach your users how to identify what is a basic help desk call and what might be a security incident.
- Your help desk staff should have more thorough training in identifying security incidents.
- This is typically not included in the IRP.

Keeping Notes

- Strange as it may seem, the first thing you should probably do is start taking notes.
- Keep detailed notes to the extent that an external investigator could completely reproduce your work.
- Write down not only what you've done, but also why you did it. Later on you might find yourself wondering why you chose to take some action.

Keeping Notes

- The IRP should specify what kind of information needs to be retained, where it is going to be retained, and if it should be encrypted or not.
- The IRP should specify how long notes and supporting documents will be retained before they are destroyed.
- The person in charge is responsible for assembling and compiling notes and supporting documents.

Keeping Notes

- Nobody ever wants to do this part, but it may be the most helpful information if you decide to investigate further – so do it now.
- The person in charge must have the authority to demand other people take notes and send them on. He or she should follow up and pester people until the notes are provided.
- The IRP should require detailed note taking from everyone involved.

What have we done so far?

- An incident has occurred.
- A well-informed user knew who to contact and brought it to your attention.
- Someone has been empowered to make decisions and lead the response.
- Everyone has stopped for a moment to take down all of the notes and supporting documents they can gather. This leads me to Subtopic 2.

Subtopic 2 - Logging

- Typically when a system is hacked, the attacker will try to clean out any log files to cover his or her tracks.
- Even if they are not successful, some servers generate so many events that you can lose information when the logs rotate.
- My advice is to have a central log server (e.g. syslog) that all of your devices send information to.

Subtopic 2 - Logging

- Since the only thing this server is doing is keeping logs, you can harden it quite a bit more than your other servers. It is unlikely that an attacker will be able to wipe logs from both the target server and the log server.
- Discussions of what to log and where to log them are typically not included in an IRP, but should be addressed elsewhere.

Logging and the IRP

- What you might consider including in your IRP is heightened logging once an incident has been detected.
- This will help to record your response to the incident, and gather additional information in the event that the incident is ongoing.
- This can be done easily on a Windows domain by creating a Security template to be used during the response.

Logging and the IRP

- You might also include recording network traffic as part of your incident response process.
- It would be impractical to record network traffic for your server at all times, but if you are implementing heightened logging, then it is probably worthwhile to use a tool like Wireshark or TCPDump to record network traffic from machines that are related to an incident.

A word of caution @ acquisition

- Stored data is subject to ECPA – Electronic Communications Privacy Act (US Federal).
- Real-time data (network capture) is subject to either:
 - Wiretap act if capturing the contents
 - Pen/Trap statute if capturing only headers (no contents)
- Talk to your legal dept or representative
- Focus your efforts on the machine(s) being investigated (don't run network trace of all campus traffic).

The Big Money Question

- What is Your goal in responding to this incident?
 - Clean it up and move on?
 - Clean it up, figure out how to prevent it, and move on?
 - Clean it up, figure out how to prevent it, find out who is responsible?
 - Clean it up, figure out how to prevent it, find out who is responsible, and seek prosecution?

The Big Money Question

- This is not a decision that should be left to one person.
- Your IRP should spell out which people will be involved in making the decision of how to respond.
- I know this seems like a waste of time, but most of the time you have plenty of it.

When to contact law enforcement.

- Most times that is a decision that you can make with other stakeholders in the organization.
- Sometimes you don't have a choice. If you find evidence of a major felony (bank fraud, child pornography) or a threat to human safety (school shooting, suicide note) then you have to contact the authorities. This brings me to Subtopic 3.

Subtopic 3 – Calling for help

- You need to make contact with the authorities before you call them for help.
- Call up the FBI office in your area and tell them what you're trying to do. They will direct you to the right person.
- Call your local police and tell them that you're developing an incident response plan. They will tell you when they need to be called and who to talk to.

When contacting law enforcement

- When you have a choice in the matter, major stakeholders should be involved in the decision to call in law enforcement.
 - Your legal department
 - Senior leadership
 - Your physical security department
 - Your public relations group.
- Your IRP should specify who you are going to notify within your organization.

Final considerations for the IRP

- The person in charge should be responsible for creating a report of the incident, the steps taken to mitigate the incident, and the lessons learned from the incident.
- The IRP should require a post-incident review meeting with senior management.
- The IRP should also specify when affected customers are going to be notified of an incident (consult with legal on this one.)

What have we done?

- An incident has occurred
- A well-informed user knew who to contact and brought it to your attention.
- Someone has been empowered to make decisions and lead the response.
- Everyone has stopped for a moment to take down all of the notes and supporting documents they can gather.

What have we done?

- We assembled a group of stakeholders from around the organization to make a decision on what kind of response to initiate. If law enforcement is going to be called, then the appropriate people have been notified.
- Now you can work with your IT staff to start mitigating the problem, and that often means gathering data to find out what happened.

Live System Acquisition

- Live System Acquisition refers to the steps you take to gather evidence from a computer that is currently running.
- I strongly recommend that you have an approved procedure in place before you have to perform evidence acquisition on a live system.
- Having a tested and approved process in place ensures that you get consistent results and will increase the weight of that evidence should it be needed in a court of law.

Objections to live analysis

- The forensic methodology: Acquire, Authenticate, and Analyze.
 - Acquire without altering or damaging
 - Authenticate that your evidence is the same as the original
 - Analyze without altering the evidence you've gathered.
- Live acquisition is a destructive process

The objections don't hold water

- Destructive forensics is not necessarily bad.
 - How can you analyze a sample of chemical residue without altering it?
 - If you can show that you know how your methods alter the evidence, you can still use it.
- If you encounter a live system, there is nothing you can do that is not destructive!
- Shutting down the computer destroys more evidence than the procedures discussed next.

A better forensic methodology

- PICL: Preserve, Investigate, Corroborate, and Log.
- Understand that your efforts will make some changes. Preserve the evidence as much as possible.
- Find places where other information will corroborate your findings.

Why perform live acquisition?

- There is really good information on that computer that will be lost when you power down the machine.
 - Artifacts in RAM
 - Active Network connections
 - Running processes and the ports associated with them

Live System Acquisition

- Don't forget what I said earlier about taking detailed notes. Write down everything you observe about the machine and everything you do to the machine.
- I also recommend that you have a second person on hand during the acquisition process to verify that you're following the procedure. This requirement should be part of your procedure.

Live System Acquisition

- Gather the most volatile data first, and then move on to the less volatile stuff.
- Start with the physical memory first, as it will change the most during this process.
- Physical memory can hold amazing artifacts that can be used by an experienced investigator to gather additional information about what happened.

Helix Live CD

- A great free tool that you can use for acquiring evidence in the Helix Live CD. This CD has a variety of forensic tools that can be used for acquiring evidence on live or dead machines.
- Available at <http://www.e-fense.com/helix/>
- You're also going to need a known good machine or drive where you can store the evidence that you gather.

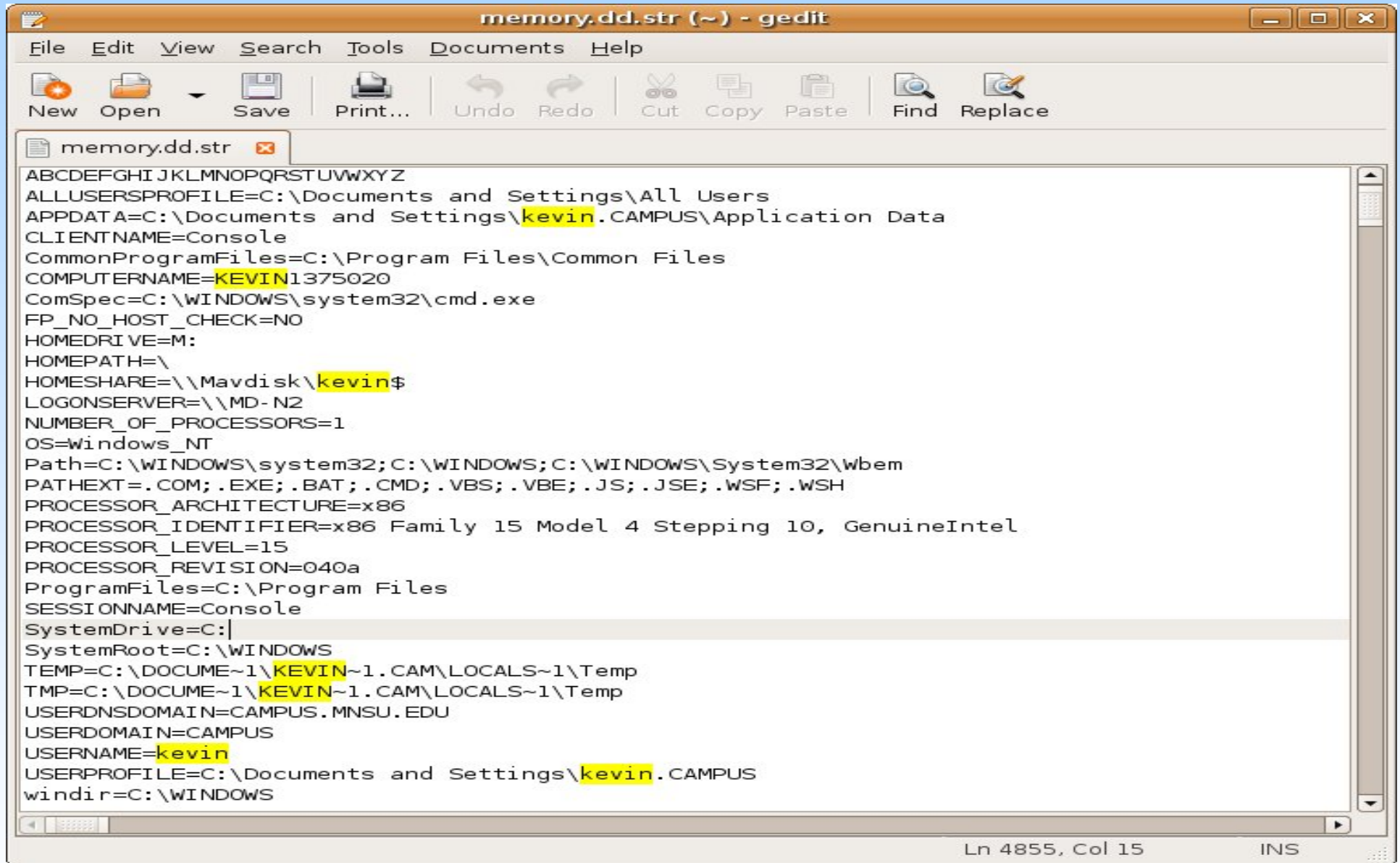
Gathering physical memory

- Insert the Helix Live CD into the suspect machine and select Live Acquisition from the menu.
- You can send a copy of the physical memory to a Windows share or use a NetCat listener on your Known Good Machine.
- Click Acquire.
- Do this before you run any other command.

What do you find in there?

- Really cool stuff
 - HTML code for pages that were recently visited
 - Registry keys that were recently read or changed
 - Strings from programs that were recently run (like the trojan horse that was used to compromise the machine)
 - Other clues about programs running on the machine (I found evidence of Open Office and VirtualBox on mine)

What do you find in there?

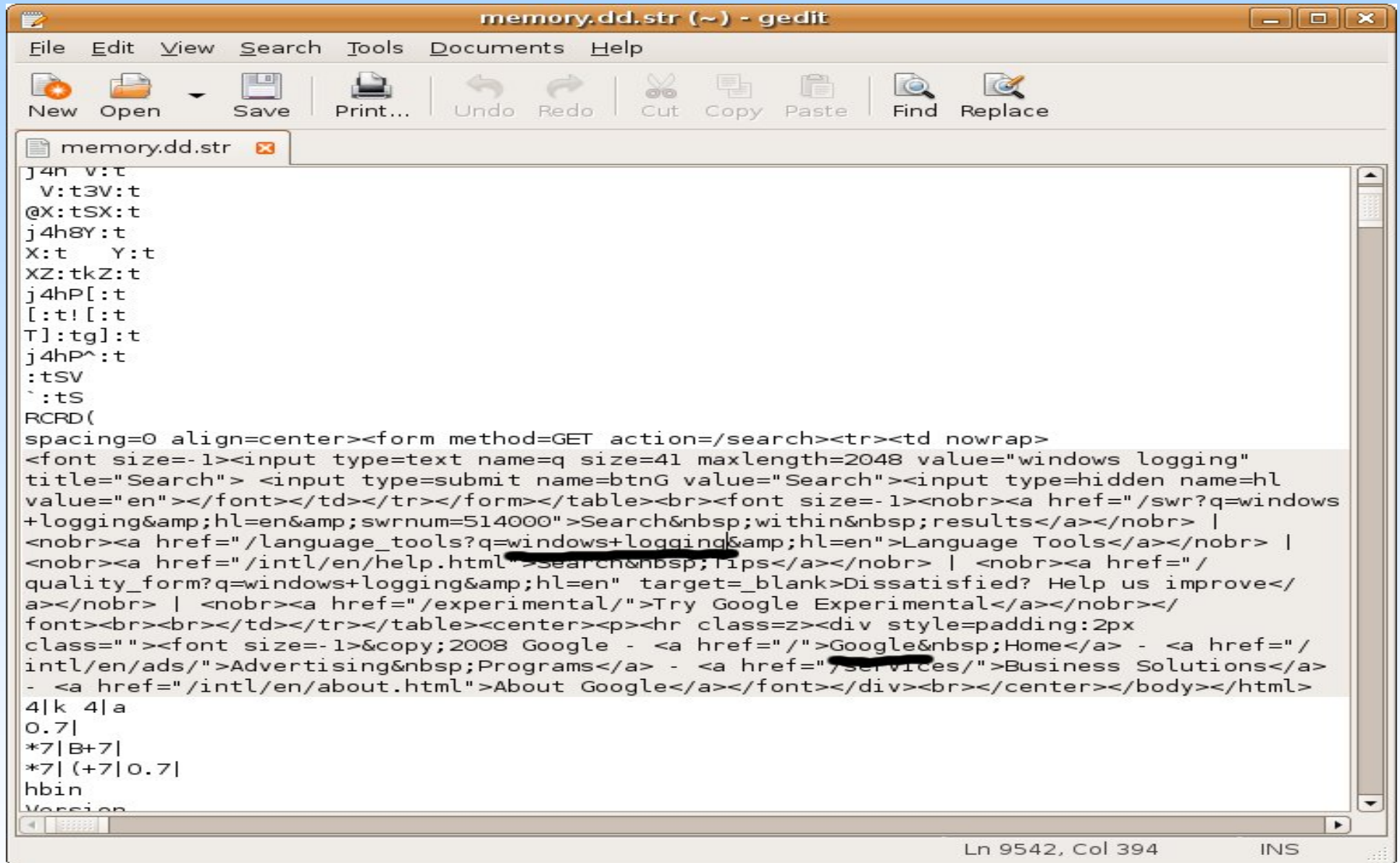


The image shows a screenshot of a gedit text editor window titled "memory.dd.str (~) - gedit". The window displays a list of system environment variables for a user named "kevin". The variables are listed in a plain text format, with some values highlighted in yellow. The variables include system paths, user information, and hardware details.

```
memory.dd.str x
ABCEFGHIJKLMNOPQRSTUVWXYZ
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\kevin.CAMPUS\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=KEVIN1375020
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=M:
HOMEPATH=\
HOMESHARE=\\Mavdisk\kevin$
LOGONSERVER=\\MD-N2
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 4 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=040a
ProgramFiles=C:\Program Files
SESSIONNAME=Console
SystemDrive=C:|
SystemRoot=C:\WINDOWS
TEMP=C:\DOCUME~1\KEVIN~1\CAM\LOCALS~1\Temp
TMP=C:\DOCUME~1\KEVIN~1\CAM\LOCALS~1\Temp
USERDNSDOMAIN=CAMPUS.MNSU.EDU
USERDOMAIN=CAMPUS
USERNAME=kevin
USERPROFILE=C:\Documents and Settings\kevin.CAMPUS
windir=C:\WINDOWS
```

Ln 4855, Col 15 INS

What do you find in there?



The image shows a gedit window titled "memory.dd.str (~) - gedit". The window contains a memory dump at the top and a large block of HTML code below. The HTML code is a search page for "windows logging" on a Google search engine. The search results section is highlighted in grey. The HTML code includes a search form, navigation links, and a footer with Google branding and links to "Advertising Programs" and "Business Solutions".

```
j4n v:t
V:t3V:t
@X:tSX:t
j4h8Y:t
X:t Y:t
XZ:tkZ:t
j4hP[:t
[:t![:t
T]:tg]:t
j4hP^:t
:tSV
`:tS
RCRD(
spacing=0 align=center><form method=GET action=/search><tr><td nowrap>
<font size=-1><input type=text name=q size=41 maxlength=2048 value="windows logging"
title="Search"> <input type=submit name=btnG value="Search"><input type=hidden name=hl
value="en"></font></td></tr></form></table><br><font size=-1><noBr><a href="/swr?q=windows
+logging&hl=en&swrnum=514000">Search&nbsp;within&nbsp;results</a></noBr> |
<noBr><a href="/language_tools?q=windows+logging&hl=en">Language Tools</a></noBr> |
<noBr><a href="/intl/en/help.html">Search&nbsp;Tips</a></noBr> | <noBr><a href="/
quality_form?q=windows+logging&hl=en" target=_blank>Dissatisfied? Help us improve</
a></noBr> | <noBr><a href="/experimental/">Try Google Experimental</a></noBr></
font><br><br></td></tr></table><center><p><hr class=z><div style=padding:2px
class=""><font size=-1>&copy;2008 Google - <a href="/">Google&nbsp;Home</a> - <a href="/
intl/en/ads/">Advertising&nbsp;Programs</a> - <a href="/services/">Business Solutions</a>
- <a href="/intl/en/about.html">About Google</a></font></div><br></center></body></html>
4|k 4|a
0.7|
*7|B+7|
*7|(+7|0.7|
hbin
Version
```

Ln 9542, Col 394 INS

Live System Acquisition

- There are other useful commands to run on a live system.
- Your Helix Live CD has a trusted command prompt that you can run.
- You should try to run all of these commands from the trusted command prompt on the CD rather than the suspect machines cmd.exe
- Make sure that you map a network drive or use a NetCat listener to capture the output of these commands

Live System Acquisition

```
date /t (note difference between machinetime and real time)
time /t
uptime
net use (display mapped drives)
net session (show sessions in progress)
net file (show open files on the server)
net share
net view
net user
net accounts
net localgroups
net start (shows running services)
nbtstat -c
nbtstat -an
arp -a
netstat -a
```

Live System Acquisition

```
psinfo /accepteula (Basic information about the OS)  
pslist /accepteula (list of running processes)  
fport (list of open ports by process id)
```

Maintaining Chain of Custody

- Once you've gathered your files, you should calculate a hash value for the files to detect any tampering.
- Put the hash values for each file in a text file and burn it to a CD (not a re-writable). Have someone else keep the CD.
- Keep track of who has access to the files and who has physical access to the CD with the hash values.

Maintaining Chain of Custody

- Do not allow any one person to have unsupervised access to the electronic evidence files and the CD at the same time.
- Do not allow the CD to leave a person's custody without being documented.
- This should all be documented in your forensic acquisition procedure.

Quick Review

- A mediocre plan is better than no plan at all.
- Create an Incident Response Plan before something happens.
 - Who is in charge
 - How to report incidents
 - What notes to take
 - Who to contact in law enforcement and when to contact them

Quick Review

- Incident Response affects many people in your organization. Make sure you include all of these stakeholders when you're drafting your IRP.
- Have an approved procedure in place describing how to acquire evidence from a running machine.
- Document the process your organization is going to use to maintain chain of custody.

Thank you