

---

**Author – Shaheem Motlekar**  
**Email – shaheem.motlekar@paladion.net**

## **Incident Handling FAQ**

The following listing of FAQs is a compilation of common questions we face while responding to incidents.

### **Suspicious processes**

- How can I list running processes in Windows?
- How do we map ports to running processes?
- Where can I get an updated list of suspicious ports?
- How can we view process statistics?
- How do I freeze a running process?
- How do I dump the contents of a running process to a file?

### **Rootkits**

- What are rootkits? How do I detect rootkits?
- I didn't prepare an MD5 database; where can I download the correct MD5 for my system?

### **MAC Times**

- Why are MAC Times relevant in IH / forensics?
- What is the difference in MAC Times between Unix and Windows?
- How can I preserve MAC Times while copying a file?
- Why is the MAC Time of the command shell important?
- How do I find out the last logged-on user?
- Where do I look for programs / commands executed at startup?

### **Hidden data**

- How do I display hidden files?
- How is data hidden in slack space?
- What are the dangers from 'alternate data streams'?
- How does Sector CRC work?

### **The coroner's toolkit (TCT)**

- Are GUI versions of TCT available?
- Where can I get a Windows version of TCT?
- How do I take a disk dump of a file for forensic analysis?
- How do I capture forensic information without overwriting the local disk?

### **Logging**

---

---

Why is remote logging recommended?

How do we send Windows logs remotely to a central server?

Which are the important log files I should be reviewing?

### **Resources**

Which are the essential IH / forensic tools that I must have in my toolkit?

How do I prepare statically linked binaries for my IH toolkit?

Which are the good books available on IH / forensics?

Where can I learn about analyzing rootkits / trojans?

---

---

## Suspicious processes

### How can I list running processes in Windows?

Running processes can be listed in Windows using a utility pslist. This is available for download at:

<http://www.sysinternals.com/ntw2k/freeware/pslist.shtml>

### How do we map ports to running processes?

In UNIX a utility called lsof (list of open ports) gives applications to open port mapping. In Linux it can be achieved using a system command: netstat -apn. In Windows the information can be found by using the fport utility from Foundstone:

<http://www.foundstone.com/knowledge/proddesc/fport.html>

### Where can I get an updated list of suspicious ports?

A good reference site is:

<http://www.doshelp.com/trojanports.htm>

Robert Graham's firewall-seen FAQs explain the meaning of the log entries in firewall logs:

<http://www.robertgraham.com/pubs/firewall-seen.html>

### How can we view process statistics?

To view process statistics in UNIX we can use the command top or sar commands. To view process statistics in Windows we can use the Windows task manager, or PsList from Sysinternals.com:<http://www.sysinternals.com/ntw2k/freeware/pslist.shtml>

### How do I freeze a running process?

The command to freeze a process in UNIX is: kill -STOP pid

### How do I dump the contents of a running process to a file?

The pcat utility in The coroner's toolkit can be used to dump the contents of a running process to a file in UNIX

## Rootkits

### What are rootkits? How do I detect rootkits?

Rootkits are used by intruders to hide and secure their presence on your system. An intruder achieves complete cloaking capability by relying on an administrator to trust the output of various system programs. This assumption is more or less true — most of the time system

---

---

administrators trust 'ps' to display all processes and 'ls' to list all files. A rootkit gets its name not because the toolbox is composed of tools to crack root, but because it comprises tools to keep root. Rootkits are detected by means of checking to see what has changed on your system. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc. A commonly used tool is tripwire.

### **I didn't prepare an MD5 database; where can I download the correct MD5 for my system?**

The correct database in the case of the Solaris operating system can be downloaded from:

<http://www.sun.com/blueprints/tools/md5.tar.Z> In Linux the command `rpm -Va` can be used to verify the integrity of all installed RPMs.

## **MAC Times**

### **Why are MAC Times relevant in IH / forensics?**

MAC Times essentially translate into modified, accessed and changed times of a file on the system.

Modification is the last time when a read or write was done to a file. Accessed is the last time a file was accessed. Changed is the last time the permissions / owner of the file was changed. From an IH perspective we need to know if an attacker has changed any binaries, configuration files to capture evidence for further forensic analysis. Dan Farmer's classic article on MAC Times is available at DDJ.

### **What is the difference in MAC Times between UNIX and Windows?**

Unlike in UNIX, when a file is copied in NTFS the mtime of the new file is the same as the original file, while the atimes and ctimes reflect the copy action. This can make a file appear as though it was created after it was modified! Also, NTFS updates the atime only if the updated atime is an hour or more later than the previous atime.

### **How can I preserve MAC Times while copying a file?**

The `-p` option in the `cp` command preserves the modified and access times of a file while it is copied in UNIX

### **Why is the MAC Time of the command shell important?**

The command shell is often spawned in buffer overflow attacks to give control to the attacker. This changes the MAC Time of the command shell, and is a good indicator of the time of the attack. During IH it's a good idea to use a different copy of the command shell than that of the system's built-in command shell, as the very act of invoking the command shell to run a MAC Time utility can change the MAC Time of the shell.

---

---

### **How do I find out the last logged-on user?**

The command 'last' can be used to find the last logged-on user in UNIX. The NTLast utility from Foundstone can be used in Windows for the same purpose.

### **Where do I look for programs / commands executed at startup?**

The location is: C:\windows\start menu\programs\startup

The registry key is: HKLM\Software\Microsoft\Windows\CurrentVersion\explorer\Shell

Folders:

"Common Startup"="C:\windows\start menu\programs\startup"

### **Hidden data**

#### **How do I display hidden files?**

Hidden files in \*nix can be displayed by the command:

Ls -al or Ls -Al.

The equivalent command in Windows is : dir /A:H

#### **How is data hidden in slack space?**

Data can be hidden in the slack area caused by file sizes that don't exactly match the size of the clusters in which they are stored. Cluster sizes can vary, but any time a file or portion of a file is smaller than the cluster size, the 'leftover' bits in that cluster go unused. In file systems such as FAT16, where cluster sizes increase based on the partition size, this can result in a very large amount of 'empty' space, and that space can be used to covertly store other bits of data.

#### **What are the dangers from 'alternate data streams' (ADS)?**

The primary reason why ADS is a security risk is because streams are almost completely hidden and represent possibly the closest thing to a perfect hiding spot in a file system — something Trojans can and will take advantage of. Streams can easily be created / written to / read from, allowing any trojan or virus author to take advantage of a hidden file area. But, while streams can easily be used, they can only be detected with specialist software. Programs such as Explorer can view normal parent files, but they can't see streams linked to such files, nor can they determine how much disk space is being used by streams. Because ADS is virtually unknown to many developers, there are very few security programs available that are ADS-aware. As such, if a virus implants itself into an ADS stream, your anti-virus software will probably not be able to detect it. In addition, streams cannot be deleted; to

---

---

delete a stream you must delete its parent. Streams are of particular importance to law-enforcement agencies since important data can sometimes be hidden in these covert file-system channels.

### **How does Sector CRC work?**

The CRC at the end of the data area of a sector is generated when a sector is written to. Subsequently, the CRC is checked when the sector is read. If the CRC value doesn't match, then it's flagged as bad and some type of error should occur. If a disk utility such as diskedit is used and the data area is changed (a line of text is added to a document) in a sector, the sector CRC does not report an error when accessing the file normally at a later time. This is because the CRC referred to is generated by the hard / firm ware on the drive / controller itself. Hence, when you edit a sector and write it back out, the CRC gets regenerated properly.

## **The coroner's toolkit (TCT)**

### **Are GUI versions of TCT available?**

The 'autopsy forensic browser' is the HTML interface to TCT and TASK. It uses the file system tools of TCT and TCTutils as a foundation. This is available at:

<http://www.atstake.com/research/tools/autopsy/>

### **Where can I get a Windows version of TCT?**

A Windows versions of TCT are available from atstake and are known as TASK. TASK is written in C and uses the file-system tools of TCT and TCTutils as a foundation. It can be downloaded at: <http://www.atstake.com/research/tools/task/>

It can be used to analyze FAT, NTFS file systems.

### **How do I take a disk dump of a file for forensic analysis?**

Disk dump of a file for forensic analysis can be taken using the dd command: DD if=/etc/configuration of=/dev/rmt/0

### **How do I capture forensic information without overwriting the local disk?**

To capture forensic information we can do a DD (disk dump) of the file system. Be careful while doing a DD because the output device should be the same size or larger than the input device. The syntax for DD is:

DD if=/dev/dsk/c0t0d0s3 of=/dev/dsk/c0t1d0s3, where 'if' is the input device, and 'of' is the output device.

---

---

## Logging

### Why is remote logging recommended?

If an attacker compromises a server, the first thing that he would do is to wipe his traces: clean out the logs on the local system that the administrator might check. If we have a central server collecting the logs, we'll have a redundant (and more secure) copy of the logs. Syslog is often used as the transport for this central logging.

### How do we send Windows logs remotely to a central server?

Configure a syslog server on a Linux box or a Solaris box to receive logs in syslog format from external servers. Install a Windows syslog agent on the Windows servers to push logs to the central syslog server. A popular Windows syslog agent is NTSyslog.

### Which are the important log files I should be reviewing?

In UNIX the log files that need to be looked at are: `/var/adm/messages`, `/var/log/messages`, `/var/log/authlog`, `/var/log/sulog`, `last`, `lastcomm`.

`/var/adm/messages` — this is where the error messages from the system are stored (kernel-related errors, file system full).

`/var/log/messages` — this is for Linux ( varies from OS to OS) and does the same as above.

`/var/log/authlog` — this file is for authenticated services like telnet, ftp.

`/var/log/sulog` — this file is for users using the "su" command to switch to another user.

`last` — this command picks up data from the `wtmpx` file (it shows what time user logged in, which ip,console or telnet).

`lastcomm` — this is a command which shows the output for process accounting if it is enabled.

`.sh_history` — last few commands executed.

## Resources

### Which are the essential IH / forensic tools that I must have in my toolkit?

Windows

`Cmd.exe` — to execute a trusted command shell.

`PsLoggedon` — a utility that shows all users connected locally or remotely.

`Rasusers` — to list users logged in via RAS.

`Netstat` — to list out the open ports.

---

---

Fport — lists the o/p of open ports to applications.

Pslist — view memory, cpu and thread statistics.

Afind — to list files which were accessed during the attack.

Nbtstat — recent connections are maintained in the cache.

Arp — displays and modifies the Internet-to-ethernet address translation tables.

Kill — the kill utility sends a signal to the process or processes specified by each pid operand.

Md5sum — to check integrity of the files.

Rmtshare — to display and share folders on a remote server.

Pwdump — to dump the password file.

Netcat / Cryptcat — use it to send data to a forensic workstation.

Regquery — reviewing key registry entries (from the NT resource kit).

Dumpevt — dump eventlog in a format suitable to importing into a database.

UNIX

Statically linked binaries·

Ps·

Ls

netstat·

ifconfig — to check if the output from the good binaries is different from the system binary.

who — list of users logged on.

LSOF — application to port mapping.

TCT — (The coroner's toolkit)· unrm· graverobber· lazarus· mactime.

MD5sum — to check the integrity of the files.

^

### **How do I prepare statically linked binaries for my IH toolkit?**

Hal Pomeranz has written an excellent guide to preparing statically linked binaries in Solaris:

<http://www.deer-run.com/~hal/sol-static.txt>

An explanation of how to create statically linked binaries in Linux is available at:

[http://www.incident-response.org/howto\\_1.htm](http://www.incident-response.org/howto_1.htm)

### **Which are the good books available on IH / forensics?**

Some of the better books on IH / forensics are:

---

---

Computer Forensics: Computer Crime Scene Investigation, by John R. Vacca and Michael Erbschloe,

Computer Forensics: Incident Response Essentials, by Warren G. Kruse II and Jay G. Heiser.

**Where can I learn about analyzing rootkits / Trojans?**

Lenny Zeltser has written an excellent article on analyzing malware at:

<http://www.zeltser.com/sans/gcih-practical/revmalw.html>

---