Computer and Internet Forensics
Assignment 2

Dylan Leigh
Student # s3017239

Semester 2 2010

Notes:

- As requested on the discussion board by the head tutor, all text from the assignment 1 report is in a different colour (green).
  - In the Table of Contents, sections with a blue or red link are entirely new, and sections with a black link have partially new and partially old content.
- Evidence that the partition was created by the head tutor on his laptop have not been included in this investigation and have not been considered when formulating any conclusions or recommendations:
  - Presence of the Linux partition (in the partition table, although not included in the disk image).
  - The partitions appear to be created by mkdosfs (a Linux tool) - they contain the OEM ID string " mkdosfs" and the mkdosfs boot message strings.
  - Uninstall shortcut for Oracle VM VirtualBox Guest Additions (implies that this software was installed and the system was a guest OS).
  - "transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2).lnk" shortcut file (the default Ubuntu system name is "<username>-laptop" and the default username is the first name of the user who installed the system).
    - The transfer shortcut also has matching registry keys.
- Due to running out of time the Web browser and Text Search sections were not analyzed in as much detail as they should be in a real forensic investigation. These sections mention this ("Due to time constraints....").

Contents

1 Background to the Case

1.1 Probable Cause

Probable Cause is a legal concept referring to a reasonable, factually based belief that something is likely. This belief must be based on evidence, facts and logical inferences from them, and not feelings or "intuition". Usually, such as in this case, "probable cause" refers specifically to the belief that it is likely that a crime was committed (or is being committed, or about to be committed).

It is unclear if a better-than-even chance is required for probable cause, although it is strongly implied. The chance of a successful prosecution is not a factor, only the belief that the crime was committed[1].

Probable cause is an important legal concept as decisions made on the basis of probable cause may involve invading a person's privacy, depriving them of their property and even detaining or arresting them. In most circumstances if a search is made without probable cause any evidence found can not be used in court. An arrest, search or prosecution made without probable cause is usually illegal.

In this case, information has been obtained from a unknown source, via a journalist. An anonymous allegation would normally not be considered probable cause for a search of private property, although the reputation of the journalist and any history of accurate reporting may imply that their sources are credible.

1.2 Search Warrant

A search warrant is usually required to enter and search private property (e.g. a home or business). Police may sometimes search premises without a warrant (e.g. if the owner and occupier give permission or they have a arrest warrant for someone on the premises). Police may also usually search any items carried by someone when arrested.[2]

Search warrants are usually obtained from a magistrate[3]. There are different types of search warrants, specified under different acts of law with different procedures for applying for them and who may issue them. For example, some special warrants specified in terrorism laws must be issued by the Supreme Court; some limited search warrants for drug offences may be issued by any court, magistrate or a Justice of the Peace. The main laws we are concerned with in this case would be the Magistrates Act 1989 (subdivision 5)[4] and the Crimes Act 1958 (part IIA)[5].

In some cases anyone can obtain search orders from a court (sometimes referred to as "Anton Piller" orders, referring to a often-cited English case[6]). Laws for search orders are very different to search warrants, although both allow for forensic investigation and seizure of evidence. Special provisions may apply to Anton Piller orders where computer evidence is obtained, including the presence of an independent computer expert and extra requirements for documentation[7][8].

Evidence must be provided (by oath or affidavit) when applying for a search warrant. The magistrate (or court or Justice, if applicable) must be satisfied from the evidence that there are reasonable grounds to believe that an offense has been or is intended to be committed and that on the premises there is or will be something relevant to the investigation of that offense.

Search warrants must usually be presented to the occupier of the premises specified in the warrant. If the premises is not currently occupied the warrant typically authorizes the police to break and enter the premises to collect evidence, without presenting it to anyone first. Usually searches must be carried out during daylight, and "search orders" must normally be served between 9AM and 2PM. Some warrants allow the police to enter secretly and/or without informing the occupier.

[1] http://www.austlii.edu.au/au/cases/cth/HCA/2007/10.html
[2] http://www.legalaid.vic.gov.au/cl.police_powers.pdf
[3] http://www.rurallaw.org.au/handbook/xml/ch09s06s02.php
[4] http://www.austlii.edu.au/au/legis/vic/consol_act/mca1989214/s75.html
[5] http://www.austlii.edu.au/au/legis/vic/consol_act/ca195882/s341.html
[6] Anton Piller KG v Manufacturing Processes Ltd & Ors [1975] http://www.bailii.org/ew/cases/EWCA/Civ/1975/12.html
[7] http://www.fedcourt.gov.au/how/practice_notes_cm11.html
[8] http://www.supremecourt.vic.gov.au/wps/wcm/connect/d4eaf7004056cc3494b0bee505682c73/PracticeNote-No2-2006_SearchOrders.pdf?M

1.2.1 Protocols and Documentation

During an investigation it is important to follow the correct protocols and document all procedures extensively as improper protocol and lack of documentation may damage the case. Many procedures although tedious are a legal requirement and not following them may be illegal for the investigators who may then be prosecuted themselves.

It must be shown that evidence was gathered by competent personnel and that it was not tampered with. Evidence gathered without the without following protocol may not be admissible in court, as the court may conclude that it was obtained illegally or may have been contaminated, tempered with or fabricated. This may result in an unsuccessful prosecution if evidence which implicates the plaintiff is thrown out.

1.3 Search & Seizure

1.3.1 Search Tasks

Note: this is a list of tasks we performed during the initial search phase of the investigation and does not include seizure procedures.

- Photograph rooms before searching - necessary to document the original state of the premises; objects may be moved or disturbed during the search. It is possible other forensic officers have already taken care of this step.
- Search for phone and fax devices - the suspect may have communicated with others involved in the crime and records may be stored on their communications equipment. These records should be compared against logs from the telecommunication provider.
- Search for removable media - the suspect may have stored any incriminating information in removable media so it would not be found if his laptop was examined. All recordable media should be examined as it may have a misleading label (e.g. a CD containing records of bank transfers labelled as “Holiday photos”).
- Search for software/hardware documentation, packages and receipts - these items may provide useful information on the software and hardware of the suspect’s system. Specialized equipment and software may require specialized forensic equipment or software.
- Search for security tokens (such as RSA fobs and one time pads). These may be required to access encrypted data on the suspect’s system or access systems of others involved in the crime.
- Check books, papers and other effects. Although not “digital” evidence these items may contain passwords and non-digital evidence such as names and addresses which will assist the digital investigation (e.g. searching media for names, numbers, addresses for more information).

1.3.2 Note regarding Digital Evidence

Digital evidence is any information in digital form that may be used as evidence in a trial or legal case. Digital evidence may be found on storage devices or captured during transmission. To be admissible as evidence the information must be legally obtained, authentic and probative (tending to prove or disprove one of the important factors of the case).

There are several advantages digital evidence has over other forms of evidence - it is easily duplicated and easily checked for manipulation. Many individuals do not have the skill to remove all traces of the data on their systems; files which have been deleted may often be restored or the information in them recovered through other means.

However, digital evidence is easily fabricated and planted which is a major disadvantage - it is often difficult or impossible to prove that the evidence is authentic. It also usually requires specialized domain knowledge to obtain digital evidence.

1.3.3 Seized Items

A USB flash disk was recovered from the suspect "John Smith". The image from this disk forms the basis of this investigation.

2 Initial Examination and Image Scan

2.1 Image copying

2.1.1 IDE/SATA Disk copy procedures

- If possible, have multiple persons present and document the process (including with photographs) to validate authenticity of the copy and chain of evidence.
- Make sure all BIOS and jumper settings for the drives are known (to reproduce drive configuration). This is especially important for a RAID configuration.
- Photograph and document anything that might be relevant, especially:
  - serial numbers
  - any unusual markings or scratches
  - all attached devices and cables
  - jumper settings.
- Remove from suspect's PC and use a "clean" host system to image the disk.
- Attach the disk to the host system via a hardware write blocker - this protects the original disk from being altered by the procedure.
- Make a copy of all drives at the lowest level possible.
  - Copy the entire drive at the bitstream level, to allow for analysis of free space and unpartitioned space as well as the partitions
  - Check for "host protected area" which may not be detected by host OS.
- Make multiple copies of the drive and record them to write-once media.
  - Verify the copies against the original
  - Consider computing digests of all data for verification now and later.
- When finished with the drive(s) ensure they are stored in a safe place where they will not be damaged or tampered with.

2.1.2 Image copying software

"dd" was used to make the image copy. dd or a similar utility should be used rather than Partimage, as Partimage only copies the sections of a partition which are marked as used. dd can be used to copy the entire device at the block level, including free space within a partition. dd can also be used to copy unpartitioned space and unrecognized partitions.

2.2 RAID Issues

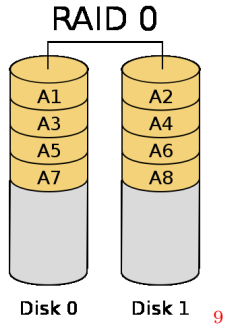
When a PC which uses RAID is analyzed, as well as taking a separate image of each of the disks the RAID configuration must be reconstructed. The configuration on the suspect PC - which may involve the OS and/or a hardware controller - must be documented fully before removing the drives.

As long as identical RAID software/hardware (whichever is applicable) can be obtained and the original setup was properly documented it can be reconstructed again on a clean system once the drives are removed. If not it may be necessary to use the suspects system for taking an image of the RAID array. This is usually not recommended as the system may be booby-trapped. It may still be possible to use a hardware write blocker to prevent alterations to the drives.

There is a possibility that data could be hidden 'outside' of the RAID array (e.g. at space at the end of a drive which is configured to not be used by the RAID software/hardware). Therefore the drives should also be independently imaged and analyzed as they would in a non-RAID system.

2.2.1 RAID 0, 2 and 5

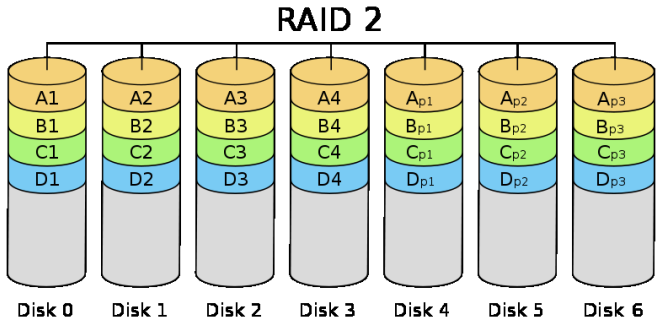
RAID 0 is also known as a "striped volume" and is a block-level form of data striping - sequential blocks are written across different physical disks. There is no redundancy and all physical drives are required to recover the volume.



[9]

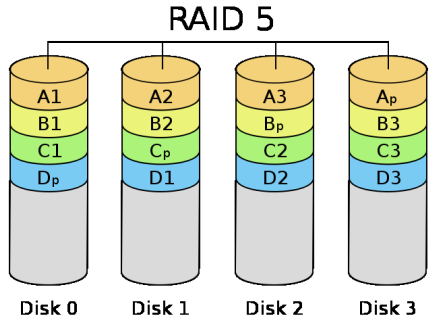
RAID 2 uses bit-level striping and hamming codes to provide error detection and correction. Each bit in a stripe including the hamming bits are stored on separate disks. A RAID 2 array therefore requires at least 3 disks, although it is extremely inefficient with 3 (one disk is used for the data bit of each stripe, two disks will be used for parity). RAID 2 is rarely used.

All data can be recovered even if any one disk is damaged or lost. As long as the data disks are intact none of the parity disks are required to recover the volume.



[10]

RAID 5 uses block level striping, with parity blocks which are distributed across all the disks. All data can be recovered if any one disk is damaged or lost. RAID 5 requires at least 3 disks. RAID 5 is popular as it provides high availability (in some systems it is possible to replace a failed disk in a RAID 5 array and rebuild the array while the system is running and the disks are being accessed).



[11]

[9] This image was reproduced from Wikipedia and was originally created by user "Cburnett". http://en.wikipedia.org/wiki/File:RAID_0.svg

[10] This image was reproduced from Wikipedia and was originally created by user "knakts". http://en.wikipedia.org/wiki/File:RAID_2.svg

[11] This image was reproduced from Wikipedia and was originally created by user "Cburnett". http://en.wikipedia.org/wiki/File:RAID_5.svg

2.3 Overview of Disk Image and Partition Table

An image of the USB flash disk was made by forensics technician Jason ("disk-image.img", MD5 hash of 2d168225bb245880232a83424c785d8c)[12] and Jason has also extracted a partition from the disk ("partition.img", MD5 hash c742e284e31dc3ead96e984d31d8623a).

The partition table of the recovered disk image is shown below (output from MMLS[13]). The Partition table, the two unallocated sections and the FAT32 partition were isolated using MMCAT (a transcript of these commands can be found in Appendix D.1 on page 47).

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
     Slot    Start        End          Length       Size    Description
00:  Meta    0000000000   0000000000   0000000001   0512B   Primary Table (#0)
01:  -----   0000000000   0000020479   0000020480   0010M   Unallocated
02:  00:00   0000020480   0000225279   0000204800   0100M   Win95 FAT32 (0x0B)
03:  -----   0000225280   0000266239   0000040960   0020M   Unallocated
04:  00:01   0000266240   0000471039   0000204800   0100M   Linux (0x83)
```

Note: Linux partition was ignored per Head Tutor's instructions - see note on cover page.

The 4 sections of the disk extracted (using MMCAT) were:

disk-part0.img (MD5 Digest 8db5fe663b6e950b37b08681e78daa4b)
The partition table. Analysis in the following subsection.

disk-part1.img (MD5 Digest 499ab331458b2a1d38c1082a467dac33)
Marked as unallocated. This part of the disk contains only null bytes. (This file also includes the partition table from "disk-part0.img" as they both start at sector 0; apart from the partition table it is empty).

disk-part2.img (Md5 Digest 1b07b235b221b2360bfdd56046ebf0b3)
Appears to be the main system partition. Analyzed in detail in following sections.
This partition has OEM ID " mkdosfs"[14] and the mkdosfs boot message; serial number serial number BECA2FE2 (hex); the volume label is present but contains only 11 space characters.

disk-part3.img (MD5 Digest 2a9dc1864f9d0791f3d8302a99e4199a)
Although marked as unallocated, this section contains a FAT16 partition. Analysis of this partition is described in section 3.2 on page 12.

[12] MD5 Digests of all files mentioned in this investigation can be found in appendix B on page 44.
[13] Details of all software used in the analysis are in appendix A.
[14] mkdosfs is a Linux tool, which implies that this partition was created by a Linux system. However, for the purposes of this assignment it is assumed that this is an artifact of the way the disk image was created by the head tutor, and not intended to affect the investigation. See note on the cover page.

3 Hidden Filesystems

3.1 Background information

3.1.1 Locating and Reading File Systems

The following table[15] shows which operating systems can be used to find and read from different file systems. (fuse) indicates that this OS may not be able to natively access that file system but can use the popular "Filesystem in USErspace" system to access it. This system is a standard component of many Linux and FreeBSD distributions.

Operating System	FAT	NTFS	EXT2/3	UFS	ZFS	HFS+
Windows	yes [#1]	yes [#1]	no	no	no	no
Linux	yes	yes	yes	some [#2]	some [#3] (fuse)	some [#4]
FreeBSD	yes	yes (fuse)	yes [#4] (fuse)	yes	yes	some [#4]
Mac OS X	yes	yes (fuse)	yes (fuse)	yes	some [#3] (fuse)	yes
Solaris	yes	yes (fuse)	yes (fuse)	yes	yes	no

#1: Any partition may be marked with a "hidden" flag in the partition table which causes it to not be displayed in the main Windows graphical shell, although it is still visible to system tools.

#2: Linux only supports older versions of UFS and has limited support for UFS2, which is the default filesystem for some versions of FreeBSD.

#3: FUSE only has limited support for ZFS.

#4: This OS has native drivers for this FS but they do not support reading the journal. This would usually be essential for examination where the system was not shut down cleanly. Note that FreeBSD can access the EXT3 journal using FUSE (see below) instead of using its built in EXT2/3 drivers.

Note that third party drivers are available to read some filesystems such as EXT2 and HFS+ on Windows but they are not widely used and cannot be relied upon to read an image.

3.1.2 Hiding a File System

Any data can be contained in a file. Any partition or file system can be copied into a file on another file system and concealed as a regular file. For example, ISO files (used when burning CDs and DVDs) contain a file system and can be mounted like any other disk partition under Unix-like systems.

A partition may also be concealed within the "free space" of another file system. For example a new system with lots of free space could be purchased and a partition and new OS install could be secretly created in the free space (while keeping it marked as "free" in the original, vendor OS. The hidden OS could then be used while leaving the vendor OS untouched. An investigator booting the system would only see the vendor OS unless they examined the free space on the disk.

These methods are recursive, for example, a file on the bootable OS may contain a file system which itself contains another hidden file system.

Note that a partition may be hidden outside a file system, for example, inside a false swap partition, in unpartitioned "empty" space or at the end of the disk in a "Host Protected Area" which is not used by the host operating system.

3.1.3 Finding a Hidden File System

It is possible to scan for "magic numbers" associated with file system headers or other data structures (e.g. UFS superblocks start with the byte sequences 19 54 01 19 or 01 19 54). This search may find many false positives, where other data may contain the same byte sequences.

For concealment, it is possible that the partition-in-a-file will be split across multiple files, or placed within a large media file (such as a DVD or another video file). This complicates recovery but the magic numbers will still appear in the file (or some of the files, if split.

[15] Information in this table was mostly obtained from the manual pages and help files of the operating systems in the list.

Some encryption systems such as "Truecrypt" encrypt a filesystem stored as a file on another FS. The file will appear to have truly random data, with no magic numbers, which makes detection difficult. These files can still be detected by analyzing their contents for randomness (e.g. Truecrypt files are highly random according to chi-square tests, whereas most files would not be very random). This analysis may be prohibitively expensive to run on all files.

The hidden file system does not have to be in any way related to the file system it is concealed within. For example, an EXT3 partition could be concealed in a file on a FAT32 partition, or a NTFS partition could be concealed on a file in a UFS2 partition.

3.2 Concealed FAT16 Partition

As already mentioned[16], a FAT16 partition was found after the main system partition, in 20 MB of space marked as "unallocated" in the partition table.

The transcript of commands used for the following analysis appears in appendix D.2 on page 48. Some hex dumps have not been included for size reasons.

This partition has OEM ID " mkdosfs"[17] and the mkdosfs boot message; serial number serial number EAC1D612 (hex); the volume label is present but contains only 11 space characters.

The file system contains only one file - "REPLICA_.JPG" with MD5 21522b41731798592433357199215fda - and no deleted files were detected. This file was extracted and analyzed further. It should be noted that the recorded modification time on "REPLICA_.JPG" is 2012-12-12 11:12:00 (EST) - this is obviously false. No creation or access times are recorded. According to FILE it is a JPEG/JFIF file. A file carver was used to check if any files had been concealed within it.

Both "REPLICA_.JPG" and the entire concealed partition was analyzed with the FOREMOST file carver. Apart from the JPEG data, a password protected RAR file was located within it. The same JPEG data and RAR files were obtained from both carves. The RAR file has MD5 digest 763da572e4cf48f699d708611c1b0bab and was given the name "00000091.rar". The JPEG and RAR files found will be discussed in more detail later (Encrypted Files, section 9 on page 20).

The file carver also detected what appeared to be BMP and EXE headers within the file; however, these seem to be false positives. Only initial headers were found (no other data structures), and their positions in the file overlap the JPEG and RAR data.

All files found by the file carver in the entire partition were also found in "REPLICA_.JPG". By looking at the partition hex dump, it can be seen that there is no data (only null bytes) after the end of "REPLICA_.JPG" and the FAT ends at the start of the file. This supports the conclusion that "REPLICA_.JPG" is the only file on this filesystem (not counting the RAR file concealed inside it).

[16] Section 2.3 on page 10

[17] mkdosfs is a Linux tool, which implies that this partition was created by a Linux system. However, for the purposes of this assignment it is assumed that this is an artifact of the way the disk image was created by the head tutor, and not intended to affect the investigation. See note on the cover page.

4 Initial File Analysis

The contents of the main section of the disk were listed using the command "fls -r disk-part2.img". As this command produces 1932 lines of output the transcript has not been reproduced in this report. Sample output is shown in appendix D.4 on page 52 which also shows the commands used to extract and analyze files mentioned later in this section.

The contents of the disk appear to be a Windows XP user directory. The directory "John S" (presumably the username of John Smith, the suspect) is the only file in the root directory; inside this directory are the usual files and directories contained within the per-user directories under "Documents and Settings" on a Windows XP system.

A number of notable files were found:

- "replica_state_license_plate.gif.lnk" was immediately noticed, significant as the "REPLICA_.JPG" on the hidden partition already investigated was an image of US state license plates. This file was within the "Recent" (recently accessed) shortcut directory.
  - A search for "state_licence" revealed what appears to be (from the filenames) a GIF file matching the shortcut (within the "My Documents" folder where users' current working files are often kept), a web shortcut (.URL file) which may be the source of the file and a deleted file entry (the deleted file will be analyzed in section 7 on page 17). The non-deleted files were extracted and MD5 digests determined:

    replica_state_license_plate.gif afb056f39ef61a1d208c08afa4c6adba

    replica_state_license_plate.gif.lnk e3f451501f42e1f130ca93241974e713

    http–headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url ece7a04cfe3b5659471ad230958b7cc2

    These files will be analyzed further in the following subsection.

- Another interesting file in the "Recent" shortcut directory was the file "Links.txt.lnk". No matching "Links.txt" file was found on the disk.
  - "Links.txt.lnk" was extracted with MD5 digest a8df937402dfce8575fe73041edd9a58
  - Further investigation reveals that Links.txt.lnk points to \\10.0.0.2\transfer\Links.txt
    - *Note: Evidence showing that 10.0.0.2 was the IP of "rohit-laptop server (Samba, Ubuntu)" have been excluded from the investigation - see note on cover page.*

- Internet Explorer history, cache and cookie files (analyzed in section 8 on page 18).
- Windows user registry files (analyzed in section 5 on page 15).
- Deleted file entries "{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf" and "replica_state_license_plate.gif " (analyzed in section 7 on page 17).
  - It should be noted here that these two deleted file entries were the only contents of the "Desktop" folder. This implies that all files on the Desktop were recently deleted - possibly this was done by the suspect after learning he was under suspicion.

- Adobe/Macromedia Flash Cookies

Note: The files "transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2).lnk", "transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2)" and the "Oracle VM VirtualBox Guest Additions" directory were not included in the analysis, see note on cover page.

4.1 replica_state_license_plate.gif and associated files

Transcript of commands used for this analysis is in appendix D.5 on page 53.

Examining the replica_state_license_plate.gif file, it was found to contain the same image as "REPLICA_.JPG", but without the circles indicating which numbers make up the password to the hidden RAR file:

It is presumably the source of the image used for "REPLICA_.JPG". The shortcut url file also found supports this theory - the same GIF file can be obtained at the URL in the shortcut.

It appears that whoever was using the system wished to conceal the RAR-encrypted "Local.txt" file. They obtained this licence plate image from the URL indicated, circled the numbers indicating the password, saved the result as a JPEG file and appended the RAR file to it.

The presence of the shortcut to the GIF file in the "Recent" folder implies that it was accessed recently. The path in the shortcut file points to the Desktop, where the deleted version of the file was (it is possible the file was very recently moved from the Desktop to "My Documents"). Timestamps on these files are analyzed in section 15 on page 27.

The GIF file was checked (with the FOREMOST carver) to see if it contained any concealed files but none were found. The other files were checked via hex dump but do not appear to contain any concealed information.

4.2 partition.img

Transcript of commands used for this analysis is in appendix D.6 on page 54.

It was observed that the partition provided by Jason did not match the partition extracted during this investigation from the (full) disk image.

The following files are different:

- The modification, creation and access times of the "My Documents" folder are different:

Source	Modify Time	Access Time	Creation Time
disk-part2.img	2012-12-12 11:12:00 (EST)	2012-12-12 00:00:00 (EST)	2010-09-08 16:06:56 (EST)
partition.img	2010-09-12 12:44:34 (EST)	2010-09-12 00:00:00 (EST)	2010-09-12 12:44:34 (EST)

- The "replica_state_license_plate.gif" file in "My Documents" has been deleted in partition.img. The modification and creation times are also different:

Source	Modify Time	Access Time	Creation Time
disk-part2.img	2012-12-12 11:12:00 (EST)	2012-12-12 00:00:00 (EST)	2010-09-08 16:06:56 (EST)
partition.img	2010-09-12 12:44:34 (EST)	2012-12-12 00:00:00 (EST)	2010-09-12 12:44:34 (EST)

- A deleted file "I9qQ5WEYf5oAV-77roMCcmqQt403aRa" is present in the "My Documents" folder in partition.img.

At this stage **the files have not been analyzed to see if their contents differ, only the files present**. There are possibly other changes in unallocated space and partition data structures which will be investigated later (see section 19 on page 33).

5 Registry Files

The transcript of commands used when analyzing the registry is in appendix D.7 on page 55. Not all of the registry contents can be reproduced due to size limitations, but most of the significant sections have been printed using GREP.

The user registry file NTUSER.DAT was located, extracted, and MD5 digest (015eead6ba2872e9eaebdbf160cd045e) determined. The registry was examined using the REGLOOKUP utility and several notable entries were found:

- References to replica_state_license_plate.gif, including:
  - A URL typed in to Internet Explorer matching the URL used to obtain the GIF file,
  - Files "C:\Documents and Settings\John S\My Documents\replica_state_license_plate.gif" and "C:\Documents and Settings\John S\Desktop\replica_state_license_plate.gif" have been saved and/or opened,
  - "Recent" accessed file references (as found in the Initial File Analysis section)
- The file "Links.txt" (which cannot be found on the disk) was recently opened in Wordpad.
- References to the deleted file "C:\Documents and Settings\John S\Desktop\{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf", which was opened and/or saved.
- The username is "John S" and computer name appears to be "JOHNS-93885B985".

No references to "Local.txt" or the RAR file were found. One deleted registry entry was recovered however it does not appear to contain any useful or significant information.

It should be noted that **all** registry keys were modified between 2010-09-05 15:02:42 and 2010-09-05 15:50:05, according to the *reglookup-timeline* tool. **It is unusual that all keys in the registry would be modified during a time period of approximately 50 minutes.** It is possible that these timestamps have been manipulated or that the system was recently installed and only used during this period.

6 Malware Scan

Both partitions were scanned for malware using the ClamAV virus scanner. No infected files were found. Transcript of the commands used can be found in appendix D.8 on page 57. Note that as part of this analysis the file system was mounted **read only** on the local system. The image file was **not** modified.

7 Deleted Files

As already mentioned in the Hidden Filesystems[18] and Initial File Analysis[19] section, no deleted files were located in the hidden FAT16 filesystem, and the main FAT32 filesystem contained two deleted file entries:

- John S/Desktop/{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf
- John S/Desktop/replica_state_license_plate.gif

(See appendix D.9 on page 58 for command transcript for this section).

The sector chains for these files have been lost so they cannot be recovered. Note that later file carving did not find any PDF file headers (see 16 on page 30) in the entire disk. It is possible that the "replica_state_license_plate.gif" is a leftover entry from the file being moved (from the Desktop to "My Documents"). As seen in section 5 (Registry Files) these files were accessed recently.

The MAC-times of the files can still be determined (this information will be analyzed further in the MAC-time Analysis section on page 27).

Note: No "Recycle Bin" directory was found in the image. On a Windows system deleted files are often moved to this location.

7.1 partition.img

As discussed in the Initial File Analysis[20] section, the partition extracted from by Jason differs from the one extracted from the provided disk image. Two more deleted files are present (see appendix D.9.1 on page 58 for command transcript):

- John S/My Documents/I9qQ5WEYf5oAV-77roMCcmqQt403aRa
- John S/My Documents/replica_state_license_plate.gif

Although the first file cannot be recovered, the "replica_state_license_plate.gif" was able to be extracted. Note that this file **was not deleted in the provided disk image**. A version including slack space was also recovered.

The undeleted "John S/My Documents/replica_state_license_plate.gif" from partition.img has the MD5 digest fe3ccd72644afd348936cd7e67c0483a - **this differs from the MD5 of the file from the same location, from disk-image.img**. The MD5 of the file with and without the slack space was the same.

The files with and without the slack space were confirmed as identical, both 57856 bytes long, which is exactly 113 512-byte sectors. The "replica_state_license_plate.gif" found in the same location in the original disk image was 57632 bytes, and occupied the same sectors on disk.

Investigating the file (via hex dump) it can be seen that **the entire file (and its slack space) has been overwritten with a pattern of 3 bytes (24, 92, 49 in hexadecimal). This pattern is one of the Guttmann method[21] patterns, used for securely erasing files**.

[18] Section 3.2 on page 12
[19] Section 4 on page 13
[20] Section 4 on page 13
[21] See http://en.wikipedia.org/wiki/Gutmann_method#Method.

8 Web Browser

Transcript for this analysis is in appendix D.11 on page 62. Note that as part of this analysis the file system was mounted **read only** on the local system. The image file was **not** modified. This mount was also used later in other analyses.

8.1 Internet Explorer Bookmarks

Apart from the shortcut "http–headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url" (already analyzed in section 4[22]), all other bookmarks appear to be those which are installed as part of Internet Explorer. The lack of any other bookmarks is unusual.

It is also unusual for "John S" to bookmark this site as having downloaded the file it is unlikely he would need to access it again. If he used the image to hide the RAR file it seems likely that he would avoid bookmarking the file to avoid drawing attention to it. There are two plausible reasons for bookmarking the file: one is that it may have been altered regularly (as some sort of covert channel). However, if this was the case, creating a bookmark would only draw attention to the covert channel which would be undesirable. The other reason is that **this file may have been bookmarked to draw attention to the image, which may have been planted as false evidence.**

The file links.txt (which was recently accessed - see 4 on page 13, but no trace of the actual file can be found on the disk) may have been used to store bookmarks ("Links"). Note that the "Links.txt" also appears in the browser history (see below).

8.2 Internet Explorer History

The PASCO tool (see appendix D.11 on page 62 for command transcript) was used to explore the Internet Explorer history files. Note that full dump of history is included in the transcript due to its importance as evidence.

Analysis of the Internet Explorer history reveals many interesting site visits including:

- Many hits on airline and airport websites, including the sites for Melbourne Airport, Quantas and airlines in Malaysia and Bangkok.
- Accesses http://www.humantrafficking.org/ and pages at that site, as well as other sites regarding human trafficking.
- Accesses DFAT (Department of Foreign Affairs and Trade) website.
- Accesses some news websites, particularly foreign ones, and particularly some sex crime stories (e.g. "http://www.bangkokpost.com/news/local/193458/spanish-sex-ring-exposed" and "http://www.mizzima.com/news two-human-traffickers-arrested-in-thailand.html"
- "file://10.0.0.2/transfer/Links.txt" - possibly the missing Links.txt file that was recently accessed.
- Login to Gmail. **Google should be subpoenaed for access to the user's email records.**
- Login to Yahoo, possibly Yahoo Messenger or Yahoo Mail. **Google should be subpoenaed for access to the user's messages and other data.** ("https://login.yahoo.com/config/login_verify2?&.src=ym")
- http://www.aic.gov.au/documents/7/B/A/{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf - this file is probably the same as the deleted file "{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf".
  - The file was downloaded (Md5 digest 95d691e7244300d88fa251e995b89d6b) - it is a article by the Australian Institute of Criminology on human trafficking.
- The licence plate GIF was accessed, both on the Desktop and in the My Documents Folder, from within Internet Explorer.

[22] See page 13

A detailed manual check of every URL visited would be advisable but could not be performed due to time constraints.

Note that all the URLs in the history files have **access times between 09/06/2010 01:02:46 and 09/06/2010 01:47:46**. The timings of some of these visits are unusual (see the conclusions subsection 21.1.5 on page 38 for details).

Note also that in the archived "MSHist012010090620100907/index.dat" history file, all the modified times of each link are exactly 10 hours ahead of the access times. This anomaly may be due to deliberate manipulation but is probably due to the archival process.

8.3 Internet Explorer Cache

The PASCO tool was used to examine the cache files. Command transcript is in appendix D.11 on page 62.

Cache entries were found with **access times between 09/06/2010 01:03:25 and 09/06/2010 01:47:46**. There were over 1707 entries in the cache, too many to check individually. However, by isolating the original host server of each cached file and sorting it was possible to see where most of the cached files came from.

No unusual hosts not already mentioned in the history section were found. References to some hosts not in the history were found but these appear to be advertising and tracking sites (which are commonly linked to from third parties) and probably not significant.

8.4 Internet Explorer Cookies

The PASCO tool was used to examine the index file and GALLETA was used to analyze the cookies themselves. Command transcript is in appendix D.11.3 on page 72.

The **cookie access times are from 09/06/2010 01:03:29 to 09/06/2010 01:47:41**. No unusual cookie contents or hosts were found; the cookies appear to be typical of that which would be produced when browsing the sites given in the history (mostly session ID and tracking cookies).

9 Encrypted Files

As already mentioned, the file "REPLICA_.JPG" (the only file inside the hidden filesystem) contained a RAR file (given the name "00000091.rar" by the file carving software; the original name is unknown).

A transcript of the commands used in the analysis for this section is contained in appendix D.3 on page 50.

The RAR file is password protected. The JPEG image contained in "REPLICA_.JPG" was examined to see if it contained a clue to the password used to encrypt the RAR file. The image is shown here:

Combinations of the circled numbers 0, 2 and 4 were used to attempt to unlock the password - the password "402" was successful and a file "Local.txt" (MD5 digest f5c51891b5506edbf8cbb60798cb7d6f) was extracted from the RAR file.

9.1 Local.txt

Examination of "Local.txt" (full contents is included in appendix C on page 45) shows that it contains a tab separated list, sorted into suburbs.

Each line contains, in order:

- A first name (appear to be all female names)
- A date (range from Jan 7, 2007 to Aug 6, 2011)
- A full name (appear to be all male names)
- A 7 character alphanumeric code (upper case letters only). The purpose and meaning of this column is unknown.
- A 2 digit number, ranges from 12 to 19 with a mean of 15.55 (meaning of this number is unknown; it is possibly age of a person).
- A 1 digit number (purpose unknown). Range from 2 to 8 with a mean average is 4.93.

These lines are sorted into sections grouped under a suburb heading. Each suburb heading contains the name of a suburb followed by its postcode.

As a sample, these are the first 3 lines of the file:

```
Fitzroy North 3068
Azalia    Apr 3, 2010   Russell Hartman   E9W5X31   12    7
Idola     Jun 6, 2011   Caesar Boyd       R6R0H01   14    3
...
```

Examination of a hex dump of Local.txt does not show any unusual or unexpected non-printing characters.

The names and addresses should be compared with records to see if they match real people in Victoria. There are some signs that the names on this list may have been generated in bulk - some of the male first names repeat, and some of them are not common names (there are two each of Buckminster, Byron, Caesar, Chandler, Eaton, Flynn, Mannix and Raphael). There are some common male names in the list that do not repeat (John, Christopher, Matthew, Nicholas, Richard). This implies that the list may have been constructed using a script that matches random first names to last names, without considering how common the names are.

10 File Extension/Type Analysis

The SORTER utility was used to detect mismatches between file type (determined by the FILE command) and the file extension (appendix D.12 on page 75 contains the transcript of commands). As well as detecting file extension/type mismatches, the tool was also used to sort all files into directories by type. These directories were used in later analyses[23].

Due to the large number of false positives caused by web cache files (including HTML, XML, script and CSS files) being identified (correctly) as "ASCII Text" with a mismatched file extension, an extra configuration file was used, adding entries for these file types. This file is shown in the command transcript.

In total, 1932 file entries were found, 84 of which were skipped as non-files (directories and other FS structures) and 29 extension mismatches were found. The files were sorted into the following categories:

- archive (3)
- audio (1)
- compress (13)
- crypto (0)
- data (14)
- disk (0)
- documents (19)
- exec (0)
- images (981)
- system (11)
- text (621)
- unknown (185)
- video (0)

No interesting mismatched files were found; the remainder were also false positives. A number of image files (GIF, JPEG and PNG) contained images of other formats, however these images were not suspicious and appear to be caused by misnamed files on web sites visited by the user. All images (regardless of name) were checked for metadata (see section 11 on the next page).

[23] see sections 11 on the next page and 18 on page 32.

11 File Metadata Analysis

11.1 Images

The image files extracted using the SORTER tool during the File Extension/Type analysis[24] were used in this section. A transcript of commands is in appendix D.16 on page 83.

All images were searched for JPEG comments using the RDJPGCOM tool. and EXIF data using the IDENTIFY tool from the GRAPHICSMAGICK suite. Note that not just those with JPEG extensions were searched, as some JPEG files had incorrect file extensions. Several files had comments left by the creating program. Many had APP12 "Ducky" segments (used by Adobe Photoshop) - two of these files had comments in the "Ducky" segment. The original locations of these files and the comments were:

- John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/100905_swanswin145[1].jpg

  ```
  Adam Goodes of the Swans (2nd left) embraces team mates Paul Bevan (cen-
  tre) and Jarrad McVeigh (left) following their defeat over the Blues dur-
  ing the AFL 1st Elimination Final between the Sydney Swans and the Carl-
  ton Blues at ANZ Stadium in Sydney on Sunday, Sept. 5, 2010. (AAP Im-
  age/Sergio Dionisio) NO ARCHIVING, EDITORIAL USE ONLY
  ```

- John S/Local Settings/Temporary Internet Files/Content.IE5/G92J0PQV/trinnysus_th[2].jpg

  ```
  From: ITV
  TRINNY AND SUSANNAH UNDRESS
  On ITV 1
  Picture shows: , (l-r) Susannah and Trinny
  ITV Picture contact - Peter Gray - 084488 13046 peter.gray@itv.com
  This photograph is (C) ITV and can only be reproduced for editorial pur-
  poses directly in connection with the programme or event men-
  tioned above, or ITV. Once made available by ITV Plc Pic-
  ture Desk, this photograph can be reproduced once only up un-
  til the TX date and noreproduction fee will be charged. Any subse-
  quent usage may incur a fee. This photograph must not be syndi-
  cated to any other publication or website, or permanently archived, with-
  out the express written permission of ITV Plc Pic-
  ture Desk. Full Terms and conditions are available on the web-
  site www.itvpictures.com
  ```

These files are from the web cache and the comments are probably from the original image files on the web. The comments are probably not significant to the investigation.

11.1.1 REPLICA_.JPG Metadata

The image file from the hidden partition was also examined for JPEG comments. None were found although a "Ducky" segment was present which implies that the image was created using Adobe Photoshop.

The RAR file hidden within did not contain any comments.

11.2 Documents

Apart from a standard set of templates no Office documents were found.

[24] See section 10 on the facing page.

12 Document and Shell History

All recent documents have already been analyzed during the initial file analysis (section 4 on page 13). There is no command shell history.

13 Thumbnail Caches

No thumbnail caches ("Thumbs.db") were found. A transcript of commands used for this search is in appendix D.10 on page 61.

14 Alternate Data Streams

The FAT32 and FAT16 filesystems on the disk image do not support alternate data streams.

15 MAC-time Analysis

The modification, access and creation times of files in the FAT32 partition were extracted with FLS and the MACTIME tool was used to determine a timeline. A transcript of commands is in appendix D.15 on page 82. Note that the times of the "REPLICA_.JPG" file on the FAT16 partition were already determined (one modification time, at 2012-12-12 11:12:00).

As already noted, some files have MAC-times set in 2012 which is clearly impossible. **It is almost certain that the times have been tampered with and cannot be relied upon to produce an accurate timeline of events.**

A simple count of all the file creation/modification/access events, sorted by date and time, is shown below:

```
Events  Date                 Time
1928 Thu Jan 01 1970 10:00:00
   2 Wed Sep 08 2010 00:00:00 (see note)
   2 Wed Sep 08 2010 15:17:22
 425 Wed Sep 08 2010 16:06:56
 402 Wed Sep 08 2010 16:06:58
 403 Wed Sep 08 2010 16:07:00
 403 Wed Sep 08 2010 16:07:02
 293 Wed Sep 08 2010 16:07:04
1926 Wed Dec 12 2012 00:00:00 (see note)
1926 Wed Dec 12 2012 11:12:00
```

Note that for access time only the date is recorded, and all the events recorded at midnight are access times of files modified during that day (note that the event counts are the same; this was confirmed by comparing the two sets of paths, which match perfectly).

Note also that events listed for Thu Jan 01 1970, 10:00:00 (Unix epoch, adjusted for AEST time zone) are probably not actual events, but entries where a zero has been recorded in a MAC-time field in the file system.

The registry[25] and web browser[26] files (history, cache, cookies) have internal timestamps. **Discrepancies between these and the MAC-times of the relevant files have been mentioned below.**

15.1 Detailed MAC-time timeline analysis

Wed Sep 08 2010 15:17:22

- Recorded access date for the deleted files "/John S/Desktop/{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.p and "/John S/Desktop/replica_state_license_plate.gif".

Wed Sep 08 2010 15:17:22

- The deleted files "/John S/Desktop/{7BA2B075-9282-4331-98A6-14080E701B2B} tandi338.pdf" and "/John S/Desktop/replica_state_license_plate.gif" were modified (possibly deleted) at this time.

Wed Sep 08 2010 16:06:56

- User directory"/John S" was created along with many Windows XP user settings files and directories (including "/John S/Recent", "/John S/Start Menu/" and "/John S/NTUSER.DAT").

[25] Section 5 on page 15.
[26] Section 8 on page 18.

  - It is unusual that these files and directories did not exist before as they are created as part of normal user account on a Windows XP system. It implies a recent reinstall, recent creation of the account or manipulation of the creation times by setting a large number of files and directories to the same time. Alternatively, it may be that all these files were copied to the USB flash disk at this time and the copying program did not copy the file creation time of the original file.
  - Note that according to the timestamps within the registry, all registry keys were modified between 2010-09-05 15:02:42 and 2010-09-05 15:50:05. The creation timestamp on the registry file is after that time period.

- "/John S/Local Settings/History", "/John S/Favorites/Links" and "/John S/Cookies" were created.
  - Again, it is unusual that these files did not exist before as they are created and accessed whenever Internet Explorer is used.
  - Note that according to the timestamps within the Internet Explorer history, cache and cookie files, the browser was being used around 1:30AM on the morning of 09/06/2010 - again, the creation timestamp of the files is after this.
- 284 Internet Explorer cache files were created.
- 58 cookie files were created.
- "/John S/Recent/Links.txt.lnk", "/John S/My Documents/replica_state_license_plate.gif", "/John S/Recent/replica_state_license_plate.gif.lnk", "/John S/Favorites/http–headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url" were created.
- Many other files created.

Wed Sep 08 2010 16:06:58

- 402 Internet Explorer cache files created.

Wed Sep 08 2010 16:07:00

- 403 Internet Explorer cache files created.

Wed Sep 08 2010 16:07:02

- 403 Internet Explorer cache files created.

Wed Sep 08 2010 16:07:04

- 216 Internet Explorer cache files created.
- 77 other files created.

Wed Dec 12 2012

- Apart from the two deleted files, **ALL files have the access date recorded as this day.**

Wed Dec 12 2012 11:12:00

- Apart from the two deleted files, **ALL files have the modification date recorded as this day.**

15.2 MACtime analysis conclusions

Barring an unknown and obscure software bug, the only explanation for **all files** (except the deleted two) having the access date on the same day in 2012 and the modification time at the exact same second in the future is that **someone has deliberately tampered with these timestamps**. The Linux/Unix "touch" command or a similar tool could have been used to change these. The internal timestamps of the registry and Internet Explorer files do not match with the file timestamps which further suggests that the file timestamps were altered.

The pattern of the creation timestamps is also unusual. **Many files were apparently created in a single second, which further suggests that these timestamps have been altered**. Also, many of these files (the user registry, start menu, bookmarks, recent shortcuts) were apparently created although these files would normally have been created as soon as the user started using the system. This also **suggests a large scale manipulation of the MAC-times.**

Alternatively it is possible that Wed Sep 08 2010 16:06:56 was when these files were copied to the USB flash disk, and the copying program did not copy the file creation time of the original file**.** However, if this is the case it does not explain why the deleted files have modification and access times before Wed Sep 08 2010 16:06:56.

The most likely explanation is that the two files "/John S/Desktop/ {7BA2B075-9282-4331-98A6-14080E701B2B}tandi338 and "/John S/Desktop/replica_state_license_plate.gif" were deleted, then someone has changed the modification, creation and access timestamps on all undeleted files to prevent and confuse forensic analysis (forgetting to change the timestamps on the files which were deleted). It is notable that this was done in such a clumsy manner (setting times to the same value, and to a value in the future which is obviously false) - **it implies either that the perpetrator was unskilled or wanted the manipulation to be obviously found by a forensic investigator**.

16 File Carving Analysis

Note: File carving analysis was already performed on the hidden FAT16 partition[27].

The FOREMOST file carver was used to analyze the entire disk image and the FAT32 partition (see appendix D.14 on page 80 for transcript of commands). 1253 files were found in the FAT32 partition, and 1255 in the entire disk (this was the expected result, as two files were found in the hidden partition).

The file carver located files of the following types on the FAT32 partition:

- jpg - 359
- gif - 622
- rif - 1 (RIFF multimedia image file format)
- htm - 128
- ole - 4
- png - 139

A full comparison of the carved files and the files extracted using the sorter was not made due to time constraints.

No PDF files were found. There appear to be no traces of the deleted file "{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf" remaining.

There is a large discrepancy in the files found using the two methods, but there are many normal reasons why this may be the case. For example the sorter does not separate files embedded in other files, such as icons in executables, or OLE segments in Office documents, images embedded in documents, etc. Also, the file carver may fail to recognize files which are fragmented.

[27] See 3.2 on page 12.

17 Unallocated and Slack Space Analysis

Note: through hex dump analysis it was already determined that there is no data in the slack or unallocated space of the hidden FAT16 partition[28].

All unallocated space and slack space from the FAT32 partition was extracted using the BLKLS tool (see appendix D.13 on page 78 for command transcript). The FOREMOST file carver was used on the extracted data blocks but no file headers were found.

Examining the slack space by hex dump reveals that a large amount is zeroed, but some contains data which may be from a spreadsheet file. It contains what appears to be some date/time format and number format definitions, and several times the string "[Red]" in present (this appears in conjunction with the dollar sign ("$") and brackets - possibly a negative currency indicator. The string "MS Sans Serif" appears several times (probably a font reference). The string "General" appears once, possibly a reference to the "General" cell format in a spreadsheet.

The unallocated space is entirely zeroed. This is somewhat unusual, and implies either a recent install, a rarely used system, or the possibility that the free space has been zeroed to prevent old data from being recovered. It is also possible that the files on this USB drive were recently copied and the user directory was not used from the USB drive (e.g. this may be a backup drive).

[28] See section 3.2 on page 12.

18 Text Searches

Due to time constraints, extensive text searches were not performed.

18.1 Candidate Word List

Case insensitive searches were made for the following terms:

- "John" and "Smith" (will also match "John Smith", "jsmith" and "John S")
- "jsmith"
- "Kayak" (from the email)
- "Links.txt" (missing file)
- "Local.txt" (from hidden, encrypted RAR file)
- "I9qQ5WEYf5oAV-77roMCcmqQt403aRa" (missing file)

"402" (the password for hidden, encrypted RAR file) was considered but produced too many matches (due to being a small string) to be of any use.

18.2 Results from Sorted Files

Command transcript is in appendix D.17 on page 85.

"I9qQ5WEYf5oAV-77roMCcmqQt403aRa", "Local.txt", "smith" and "kayak" received no matches.

"links.txt" matched the registry file (expected).

"John" found a large number of false positives and a number of already expected files (including the registry). This search also matched a log file which seems to show that Internet Explorer was executed on 09/06/2010 01:02:52.

19 partition.img Hex Analysis

As already mentioned in several sections there were differences found in the FAT32 partition extracted from the disk-image.img file and the partition.img file supplied by Jason. A direct comparison by hex dump of the two files follows, to ensure that all alterations of the evidence are tracked down (all offsets are in hexadecimal):

- Offset 3e0: Two bytes have been changed, possibly the free sector count (244423 to 244536).
- Offset 4040: First FAT table - appears to be the entries removed for the deleted file.
- Offset 12b640: Second FAT table - appears to be the entries removed for the deleted file.
- Offset 252ee0: Sector 4759: Changes to "My Documents" entry in "John S" directory (MACtime change).
- Offset 253f80: Sector 4767: Changes to the "My Documents" directory.
- Offset 254800: The "John S/My Documents/replica_state_license_plate.gif" file has been deleted and the data replaced with the Guttmann pattern.

These are all consistent with the changes already noticed (refer to section 7.1 on page 17 for details).

20 Client Specific Queries and Analysis

20.1 Note regarding Inode Code Values

4000 Set-user-ID. When executed the effective process user ID is set to the file owner.

2000 Set-group-ID. When executed the effective process user ID is set to the file owner. If set on a directory new files created in the directory take on the group of the directory.

1000 Sticky bit. In most file systems when set on a directory the sticky bit restricts file deletion within that directory to processes with the same user ID as the file or the directory. It typically has no effect on non-directory files. In some file systems it has a special effect and can only be set on files by the super-user.

0400 Read by owner. If this is the only bit set, the file can be read only by a process with the user ID of the owner, and cannot be written to or executed by any process.

0020 Write by group. If this is the only bit set, the file can be written to only by a process with the same group ID but not the same user ID, and cannot be written to or executed by any process. Note that as user, group and "other" permissions are read in that order, a process with the same user ID as the file may not write to it even if it does have the same group ID.

0001 Execute by other. ("Other" means a process which does not match the user ID or group ID of the file). If a directory it can be traversed by "other" processes. If this is the only bit set the file can only be executed/traversed by processes which do NOT match the file user ID or group ID.

Note that a privileged process (super-user user ID or the CAP_FOWNER capability) can override the permissions checks above (for the 1000, 0400, 0020, 0001 code values).

20.2 Email analysis

To be used as evidence we must prove that the email is genuine (not likely forged) and that the sender was somehow involved in the crime (although not necessarily a suspect or victim). Content in the email may be considered "hearsay" and not admissible as court evidence, although it may be sufficient as evidence to suggest that two individuals were in contact with each other.

The mail server operators at Google (Gmail), Yahoo and possibly Kayak should be subpoenaed for server logs and other information about this email and other emails from the two users. Yahoo's server logs, if admissible in court, may show that the email.kayak.com server really did send the message. Alternatively, it is possible but less likely that someone (possibly at or via Yahoo) forged the email from Kayak.

20.2.1 Email headers

The following headers are contained in the email. Note that **any of these headers could have been forged**, and the entire message may be a fake.

Content-type: The MIME type for the message (probably not useful).

Mime-version: The MIME version for the message (probably not useful).

List-unsubscribe: Usually contains a address which a mail client can use to unsubscribe from a mailing list. The presence of this header implies a mailing list message, but the message content seems to be for an individual. A possible explanation for this discrepancy is that this message is a forgery and the headers were copied from a mailing list post.

X-evolution-source: Added by the evolution mail client, this shows where and how the mail client received the email.

Return-path: Where to send delivery failure messages to.

Received: These headers show which servers received the message, and where they received it from. These are useful for tracing the apparent path a message took when delivered (see 20.2.2 for the path of this email).

Authentication-results: This header summarizes the results of authentication via SPF and DKIM (see below).

Domainkey-signature and Dkim-signature: This signature can be used to verify that a message was sent from a mailserver at a specified domain. Unfortunately for this investigation DKIM keys may change frequently as the system is designed only to be used for verification when a message is being delivered.
Yahoo and Kayak both add a signature; the Yahoo one is passed by the Gmail server but the Kayak one is not recognized by the Yahoo server.

Message-id: The message ID should be unique for every message (theoretically every email and news post should have a unique message ID). It is not changed when the messages have headers altered or removed during message delivery. The message ID is essential when examining server logs to verify the authenticity of the message.

Reply-to: Where the recipient should send any replies. Usually matches the from: header. Unusually, this header is the same as the message ID. This may be due to manipulation or forgery of the email; it is unlikely to be a valid email address.

X-header-versions: Purpose unknown, the same value as the reply-to and message ID headers.

To: smith_john@yahoo.com Email was originally sent to this address (may have been forged to conceal the SPF authentication failure).

Delivered-to: johnrsmith@gmail.com Email was delivered to this address.

X-yahoo-forwarded: from smith_john@yahoo.com to johnrsmith@gmail.com These three headers imply that John Smith has email accounts on Yahoo and Gmail (and his Yahoo account forwards to his Gmail account). Yahoo and Google could be contacted (or subpoenaed if required) to obtain server logs to corroborate this email and analyze other communications.

Received-spf: Sender Policy Framework headers, in this case indicating that mta166.mail.sp2.yahoo.com is not a designated sender of email from email.kayak.com. This may indicate a spoofed email (Yahoo faking an email from Kayak) but is more likely to be an artifact of the email for smith_john@yahoo.com being forwarded to gmail.

X-originating-ip: The originating IP of the message. This may have been forged or tampered in transit, but if it is accurate, the originating machine is kayak-148.kayak.tracker.postdirect.com.

Date: The date the message was (apparently) sent.

From: Intended to show who sent the email but often forged and cannot be relied upon. Unusually, does not match the reply-to address (there are often valid reasons for this, such as when the person sending a message wishes replies to go to a mailing list or another person, but this does not appear to be the case).

Subject: like the main body of the email, this may provide context as evidence

The following headers serve an unknown purpose:

- X-header-companydbusername

- X-header-masterid
- X-vitals
- X-ymailisg

20.2.2 Received Header Analysis

The following table shows the path the message took to be delivered as reported by the "Received" headers in the email. The last receiver is at the top of the table, the sender should be at the bottom **(if the headers can be trusted)**. The "hop" column indicates the receiver, the "from" column indicates where the receiver states it received the message from. The lookup columns are the results of DNS lookups (normal or reverse, a applicable) on the hop/from columns.

Hop (received by)	Hop Lookup	From	From Lookup	Notes
10.231.14.68	(private LAN address)	(none specified)		#1
10.142.164.14	(private LAN address)	(none specified)		#1
mx.google.com	(not found)	mta166.mail.sp2.yahoo.com	98.137.54.194	
(none specified)		(none specified)		#2
mta166.mail.sp2.yahoo.com	98.137.54.194	127.0.0.1 (EHLO 206.165.242.148)	(localhost) (EHLO kayak-148.kayak .tracker.postdirect.com)	#3

#1: The two private IPs seem to be servers internal to Gmail.

#2: Qmail was "invoked by uid 6007". No address is specified for current hop for this header. This was probably sent internally at the Yahoo mail server.

#3: The EHLO specified address could be forged. It could simply be an artifact of the way the message was transferred to the Yahoo server. It may also be normal if the message was sent via Yahoo webmail, with the "from" address inserted by the sender.

21 Conclusions and Recommendations

21.1 Summary of Issues

21.1.1 MACtime anomalies

Section 15.2 on page 29 summarizes the MAC-time anomalies and provides some plausible explanations. The summary is repeated here:

The most likely explanation is that the two files "/John S/Desktop/ {7BA2B075-9282-4331-98A6-14080E701B2B}tandi338 and "/John S/Desktop/replica_state_license_plate.gif" were deleted, then someone has changed the modification, creation and access timestamps on all undeleted files to prevent and confuse forensic analysis (forgetting to change the timestamps on the files which were deleted). It is notable that this was done in such a clumsy manner (setting times to the same value, and to a value in the future which is obviously false) - **it implies either that the perpetrator was unskilled or wanted the manipulation to be obviously found by a forensic investigator**.

21.1.2 Evidence of Concealment/Obscurement

Obvious attempts have been made to hide data and make forensic examination more difficult.

- The hidden FAT16 partition;
- Concealment of the RAR file at the end of "REPLICA_.JPG";
- Encryption of the RAR file;
- Alteration of the modification/creation/access times;
- Scrubbing of the "replica_state_license_plate.gif" file (in partition.img only).

The lack of some data also suggests that it some have been deleted to avoid detection (e.g. zeroed unallocated space, scarce browsing history, few files on Desktop or in "My Documents") although there are other plausible explanations for this.

21.1.3 Local.txt

The file local.txt (analyzed in section 9.1 on page 20 and reproduced in appendix C on page 45) is extremely important to the case. If genuine, it may represent a set of new suspects who may provide a great deal more information on the case. If false (possible, see section 9.1) it is highly likely that this list was planted to falsely implicate John Smith.

The genuineness of the list should be tested by **comparing the names with records of the residents of the suburbs indicated in the file to see if any matches are found. It may be significant that one of the names of the file is "Jason**", the name of the other forensic investigator on this case. However, Jason is a common name.

21.1.4 REPLICA_.JPG and RAR file

The Local.txt list was compressed in a password-protected RAR file, which was itself appended to an image with hints of the password.

Based on other files and evidence found, it appears that whoever when whoever was using the system wished to conceal the RAR-encrypted "Local.txt" file. On 6 September 2010 01:46:27 they obtained the licence plate image from http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif. circled the numbers indicating the password, saved the result as a JPEG file and appended the RAR file to it. The time given assumes that the times in the Internet Explorer history are correct.

Given the effort taken to hide the file it is unusual that the password would be so simple, and that obvious hints for the password are contained within the file. There are a few possible explanations for this discrepancy:

- The REPLICA_.JPG file was sent to John Smith with the intention to provide him with the information.
  - In this case, there would be no need to obtain the GIF file used to create the JPEG image.
- Jason, while investigating the case, used the suspect's machine to find the GIF file used to create the image.
  - Jason, as a forensics investigator, should know not do this on the suspect's machine to avoid tainting evidence.
  - Once Jason had found the file there would be no need to delete it.
  - Jason would surely have mentioned this (as well as the hidden partition) when handing over the case.
- The file was planted (false evidence) to incriminate John Smith and was given a weak password (and hints to the weak password) so that it could be easily uncovered.
  - This appears to be the most likely scenario.

21.1.5 Web Browser History

The pattern of Web Browsing is unusual. After two default pages are loaded (NB: "ninemsn.com.au" is the home page for default IE systems in Australia) the file Links.txt is accessed from a local IP address (10.0.0.2) at 01:27 on the 6th of September 2010. According to the registry, Links.txt is opened in Wordpad.

After that a number of suspicious-looking pages are visited quickly, regarding airport and airline information (01:27 to 01:35), human trafficking (01:36 to 01:41). A Gmail login is made at 01:42.

It is possible that the links visited were copied across to the system by an attacker who wished to establish an incriminating web history. This would explain the "Links.txt" file (which was deleted and no trace found in the filesystem, although the Recent Documents shortcut remained) and the unusual pattern of web browsing.

21.1.6 File Registry and Disk anomalies

There appear to be no working files on the system (in Desktop or "My Documents") apart from those which look suspicious and are directly related to the case (such as replica_state_license_plate.gif). This is unusual as it is unlikely the suspect would not be doing anything non-incriminating with his computer.

All registry keys were modified between 2010-09-05 15:02:42 and 2010-09-05 15:50:05. It is possible that these timestamps have been manipulated or that the system was recently installed and only used during this period.

All unallocated space on the FAT32 partition was zeroed. This is somewhat unusual, and implies either a recent install, a rarely used system, or the possibility that the free space has been zeroed to prevent old data from being recovered. It is also possible that the files on this USB drive were recently copied and the user directory was not used from the USB drive (e.g. this may be a backup drive).

A recently installed system would explain these anomalies, as well as the lack of web browsing history.

21.1.7 Evidence of constructed evidence

A number of things suggest the evidence and possibly the entire system has been constructed in order to falsely implicate John Smith.

- All registry entries created on the 5th September 2010, between 15:02 and 15:50.
- Anomalies in browsing history, registry, unallocated space and log files imply a freshly installed system.

  - The files may also have been copied do the USB drive recently as a backup, this would explain the zeroed free space.

- All Bookmarks, Web Browsing and Desktop/"My Documents" files found appear to be related to the human trafficking case. It is more likely a real suspect would be also doing other things with his PC (games, innocuous web browsing, etc).
- RAR file too easily decrypted.
- Unusual browsing history after obtaining "Links.txt" from a local system.
- Limited evidence that the Local.txt "evidence" was generated using random names from a list.
- Modification, Access and Creation times on files obviously altered.
  - This may be an attempt to cover up a recently installed system or a system "constructed" by hand for false evidence.

21.1.8 Differences between partition.img and disk-image.img

The differences between the "partition.img" extracted by Jason and the partition extracted during this investigation have been analyzed in detail[29].

Based on the evidence presented in section 7.1 - that a file present in disk-image.img was deleted and wiped using a secure deletion algorithm in partition.img - the only plausible explanation is that Jason has deliberately wiped this file. **This means that Jason has tampered with the evidence in this case.** Reasons for doing so are unknown, it is possible that he was attempting to conceal the evidence, also possible that he planted the evidence and was attempting to conceal this.

There is no plausible scenario where Jason did not deliberately wipe the file - if it was originally deleted and scrubbed with the 24, 92, 49 bit pattern, then he could not have undeleted the file in place, and he would have had to do this to disk-image.img *after* extracting partition.img from it.

Note that the disk-image.img file was also supplied by Jason, so it should also be considered tainted evidence in the John Smith case.

21.2 Email conclusions

The email which was analyzed may be genuine or may be forged. Even if it is genuine it does not suggest any criminal activity by John Smith or "Kayak". Although there is some evidence to suggest that it may be forged, there are plausible alternative explanations for these discrepancies, and there is not enough evidence to be conclusive:

- The domainkey signature from the Kayak server was not verified by the Yahoo server.
  - This may be due to a difference in the way sendmail and Yahoo handle the DKIM system.
- The SPF records indicate that Yahoo was not authorized to deliver emails from the Kayak server.
  - This is probably due to a known problem with SPF failing when forwarding emails (this should be verified by checking to see if smith_john@yahoo.com really forwards to John Smith's gmail account).
- The Yahoo server lists the IP address of the localhost in the received header, with the Kayak mail server entered during the SMTP transaction. This could be an attempt to forge the message as coming from the Kayak server when it did not.
  - This may be normal behaviour for the Yahoo server (the Yahoo staff should be contacted to see if this is the case)

[29] sections 4.2 on page 14, 7.1 on page 17and 19 on page 33

- The reply-to and list-unsubscribe headers are unusual (while strange this is insufficient evidence to consider the message a forgery).

The most plausible scenario is that the journalist or the journalist's source has accused someone who has no connection to human trafficking. This may be out of malice or for revenge, or possibly at random to provide extra material for a news story. If the email is forged it is possible that the journalist and/or their source forged it to add evidence to the accusation.

It may be worth considering investigation of the journalist regarding a false accusation; this should start with contacting Yahoo and Google staff and requesting server logs to verify the authenticity of the email.

21.3 Final Conclusions

Based on the Summary of Issues above (on page 37) **it is clear that Jason has tampered with the evidence of this case. Given that a file was wiped with a secure deletion algorithm this is almost certainly deliberate.**

Jason's reasons for wiping the GIF file are unknown. There are two significant possibilities:

- **Jason is attempting to cover up evidence in the case against John Smith.**
- **Jason is attempting to falsify evidence to implicate John Smith.**

If attempting to cover up evidence it is likely that Jason would have deleted other files and traces of criminal activity. It is possible that he did not have the skills or the time to properly remove them. However, if he had known why the GIF file was suspect he would probably have known of the existence of the hidden JPEG file, and deleted that from the records as well. Also, the timestamps are very obviously tampered with - files modified 2 years in the future would certainly arouse suspicion.

The second possibility is more likely - the only unusual aspect is that Jason did not wipe the file in the disk-image.img file as well. It is possible that he extracted the disk-image file before remembering to wipe the file, then created the partition.img file directly from the disk, thinking that the other investigators would only use the partition.img file he obtained rather than extract a copy of the FAT32 partition themselves. It is also possible that he knew how to scrub a file from within a FAT32 partition but not a disk partition with multiple volumes.

Given that most of the "evidence" appears to be falsified, it appears most likely that Jason falsified the evidence (as a forensic investigator he would have the skills required to "construct" false evidence). The clumsy MAC-time changes were an attempt to make it look as if the unskilled system owner was covering something up, and the GIF file was wiped to cover up the fact that he created the JPEG image himself on the suspect's system. **However, the only certain thing is that Jason has tampered with the evidence in a criminal case; as an investigator this is a serious crime.**

It should be noted that John Smith is still a suspect; however, most of the evidence (and the chain of custody of the evidence) pointing to this is suspect. All of the "evidence" may have been planted. Further evidence will be required before it can be ascertained if he has committed any crimes or is innocent. As currently there is no untainted evidence against him, it may not be possible to continue the case. The outcome of the two cases are closely linked; if Jason was attempting to cover up a crime of John Smith's it suggests that John Smith may be involved

21.3.1 Timeline

An accurate timeline cannot be generated as many of the timestamps in the system have been tampered with and many contradict each other.

21.4 Recommendations

- The chain of custody of evidence in this case is suspect; as such, all media and evidence for the case involving John Smith which was collected should be immediately checked for tampering.
  - Checks should be made against evidence **verifiable before Jason entered the chain of custody, as anything which was seized or analyzed by him is now suspect.**
  - In particular, check any activity during times that Jason was involved during the case (e.g. web history).
  - Note: It is likely that this evidence can no longer be used in a case against John Smith, but if the alterations to the evidence by Jason were deliberate falsification it is now important evidence in the case against Jason.
- Server logs should be requested from Google and Yahoo to check the authenticity of the email investigated. John Smith's emails could also be requested and investigated.

- Records of the residents of the suburbs indicated in the "Local.txt" file to see if any matches are found with real residents.
  - Jason's address should be compared with that of Jason Valentine of Richmond (from the Local.txt file).
- Jason's equipment and media should be seized and examined for evidence of tampering with this investigation (and possibly others) and any evidence that he has planted false evidence on John Smith's systems.
- Detectives should investigate if there is any link between Jason and John Smith (keeping in mind that they may be conspirators or they may be hostile).

21.5 Unresolved Issues

- The origin and purpose of the deleted file "John S/My Documents/I9qQ5WEYf5oAV-77roMCcmqQt403aRa" (on partition.img only) is unknown.
- The purpose of some of the columns in the Local.txt file is unknown. If it is false evidence it is possible that there is no purpose and the columns are simply a red herring.

Appendices

A Forensic Software used in this Investigation

The following forensic software was used in this investigation:

The Sleuth Kit - http://www.sleuthkit.org/
A kit of command line forensic tools for investigating volumes such as partitions and disk images.

- The following tools, used in this investigation, are part of *The Sleuth Kit*: MMLS, MMCAT, MMSTAT, FLS, FSSTAT, ICAT, IFIND, ILS, ISTAT, BLKLS, BLKSTAT, BLKCALC , MACTIME, SORTER.

Foremost - http://foremost.sourceforge.net/
A file carver originally developed by agents from the United States Air Force Office of Special Investigations.

reglookup - http://projects.sentinelchicken.org/reglookup/
A command line utility for reading and querying Windows NT-based registries.

rdjpgcom - http://www.ijg.org/
Displays comments in JPEG/JFIF files.

pasco - http://www.foundstone.com/us/resources/proddesc/pasco.htm
A tool for examining Internet Explorer history files, including index.dat files used in the cache and cookie stores.

galleta - http://www.foundstone.com/us/resources/proddesc/galleta.htm
A tool for examining Internet Explorer cookie files.

clamav - http://www.clamav.net/lang/en/
Clam AntiVirus is an open source anti-virus toolkit for UNIX systems.

GraphicsMagick - http://www.graphicsmagick.org/
A collection of tools and libraries for reading, writing, examining and manipulating images.

B Digests

These are the MD5 digests of all significant files used in the investigation.

```
2d168225bb245880232a83424c785d8c disk-image.img
c742e284e31dc3ead96e984d31d8623a partition.img
8db5fe663b6e950b37b08681e78daa4b disk-part0.img
499ab331458b2a1d38c1082a467dac33 disk-part1.img
1b07b235b221b2360bfdd56046ebf0b3 disk-part2.img
2a9dc1864f9d0791f3d8302a99e4199a disk-part3.img
21522b41731798592433357199215fda REPLICA_.JPG
763da572e4cf48f699d708611c1b0bab 00000091.rar
f5c51891b5506edbf8cbb60798cb7d6f Local.txt
e3f451501f42e1f130ca93241974e713 replica_state_license_plate.gif.lnk
afb056f39ef61a1d208c08afa4c6adba replica_state_license_plate.gif
ece7a04cfe3b5659471ad230958b7cc2 http--headsteadi.com-wp-content-uploads-
2008-04-replica_state_license_plate.gif.url
a8df937402dfce8575fe73041edd9a58  Links.txt.lnk
015eead6ba2872e9eaebdbf160cd045e  NTUSER.DAT
fe3ccd72644afd348936cd7e67c0483a  replica_state_license_plate.gif.from-
partition.img
b5d9bfbe936a2daa68ee2967f9a6af72  disk-part2.slack
225f2027951ede69c506d5d75768f8ed  disk-part2.unalloc
95d691e7244300d88fa251e995b89d6b  {7BA2B075-9282-4331-98A6-
14080E701B2B}tandi338.pdf
```

C Local.txt

```
Fitzroy North 3068
Azalia Apr 3, 2010 Russell Hartman E9W5X31 12 7
Idola Jun 6, 2011 Caesar Boyd R6ROH01 14 3
Rhona Oct 3, 2008 Burke Fitzgerald H0P4E86 15 7
Lacy Sep 6, 2009 Conan Ward O5A7X51 19 8
Darrel Dec 28, 2007 Keith Decker R7D2F67 15 6
MacKensie Jan 18, 2010 Allistair Moran H9E4W37 13 5
Carissa Jun 5, 2008 Lance Cobb L8U1F24 19 3
Cleo Nov 30, 2010 Tyrone Goodman Q7R3Z86 18 3
Vivien Sep 15, 2009 Xenos Solomon C2D5C44 17 5
Chastity Oct 4, 2007 Buckminster Singleton O1T2Y18 18 2
Maya Oct 23, 2009 Byron Stuart D2I6X70 18 2
Aileen May 13, 2009 Matthew Lindsey H6Q0L20 14 4
Madison May 17, 2007 Hakeem Ellis F3Z2C26 12 7
Winter May 2, 2010 Jarrod Young B9G0G01 14 6
Grace Aug 6, 2011 Aidan Horn O1R2D34 19 6
Alisa Mar 10, 2011 Raphael Mann D0Q2I15 16 7


Richmond 3121
Chanda Jan 25, 2009 Edan Callahan K4M8K52 17 6
Miriam Dec 15, 2010 Tyler Craft X2J4U65 18 5
Rhona Mar 29, 2008 Keane Stout R9K8R99 17 7
Adria Mar 21, 2010 Zachery Small K7M0P67 18 4
Kirsten Aug 20, 2007 Henry Landry K1K3W81 13 3
Ignacia Apr 5, 2010 Mannix Whitney J2R1C70 14 8
Kiara Aug 31, 2007 Byron Haney W0G0D19 18 5
Uma May 11, 2010 Mufutau Terrell C7Q1C27 16 2
Nina Jan 22, 2009 Thane Carpenter S0I6V53 12 4
Amelia Jan 7, 2007 Edward Simmons F4B9Z46 16 2
Mira Jul 10, 2007 Jason Valentine G3K6K45 17 7
Montana Jul 3, 2010 Rafael Stanton Q7H3H58 17 6
Jemima Dec 31, 2009 Clinton Moody C6C6J56 14 6
Eleanor Mar 6, 2007 Keaton Edwards O8U4P38 19 7
Alea Jan 24, 2007 Kennan Shields Q9J2G32 14 5
Rebekah Nov 29, 2007 Ivan Hoffman G0T1Z28 12 5
Regina Jun 26, 2010 Eaton Banks B5I3Y23 14 4
Kitra Jan 27, 2009 Kareem Brewer Q5I4Q42 15 7
Jillian Dec 29, 2007 Jermaine Lucas T4V1U30 17 3
Phoebe Jul 15, 2008 Mannix Keith F2Y4U50 19 6
Ciara Feb 15, 2011 Alec Levine H8W4N49 16 8


Heidelberg 3084
Lacey Sep 10, 2008 Aquila Cook Z8U0U71 19 7
Nita Apr 21, 2009 John Avery C0M0Q01 15 2
Ursa Apr 25, 2007 Ronan Meadows A6J1O58 13 6
Rama Nov 23, 2009 Buckminster Simmons V7X0E29 18 8
Carissa Mar 6, 2008 Flynn Miller H9F1C16 15 2
Jenna Sep 18, 2008 Nicholas Leonard L8V3S03 14 6
Mara May 5, 2011 Felix Hill T4P4V42 16 8
Urielle Oct 20, 2009 Quinlan Mckee I4Q6V87 15 6
Kay Jun 30, 2007 Warren Mullen Y8B1L03 17 8
Rina Sep 30, 2007 Jerome Ortiz L3M1T63 15 3
Riley Apr 7, 2010 Logan Conway Z0H3T85 13 8
Lois Feb 1, 2010 Ivor Hood T2B0R49 13 4
Anika Aug 21, 2009 Jarrod Quinn K2P9L95 17 3
Ivy Oct 19, 2009 Ivor Calderon N1O4H82 16 4
Idona Apr 7, 2011 Jameson Gibson J9H9Q36 14 4
Xaviera May 11, 2010 Keith Ball L8W7K84 15 3
Kiara Dec 4, 2008 Christopher Pitts L8C1D10 15 7
Abra Feb 8, 2011 Vernon Sheppard T3Q2S40 18 4
Leandra Mar 5, 2007 Eaton Bridges S4G7X82 18 7
Brielle Dec 15, 2010 Macaulay Estrada J3S3E26 15 7
Mia Nov 14, 2010 Seth Roth L7P7O91 14 5
Sandra Mar 1, 2010 Herman Wilder F6G8C69 16 7
Nora Jan 14, 2008 Wayne Lynch L5N5X80 19 8
Glenna Feb 6, 2011 Chandler Harding E2B0W64 12 2
```

Footscray 3011
April Feb 17, 2008 Caesar Ashley QOW6Y17 12 2
Regina Aug 21, 2008 Quamar Morrow W6H3R19 16 3
Kessie Nov 9, 2009 Rogan Allison D7E8W41 12 4
Rebecca Jul 27, 2008 Benedict Meyers C7V0J67 15 7
Candace Jul 8, 2008 Aristotle Shepherd B9I2A48 17 5
Debra Mar 18, 2007 Charles Hurst I5C0C55 17 7
Penelope Sep 23, 2009 Quentin Lindsay Z7Z8M31 15 6
Allegra May 14, 2009 Gil Oneill B4G5F83 16 6
Darrel Oct 19, 2007 Raphael Fields C2Q2U08 19 3
Tara Mar 19, 2008 Kirk Jacobson M7H8I70 12 7
Hilary Mar 18, 2010 Callum Fry Q9K5W22 15 3
Jane Mar 26, 2011 Orlando Golden H0D3F24 16 2
Kaitlin Mar 30, 2009 Harper Alvarez A2G2R26 14 7
Whilemina Mar 22, 2009 Garrison Schroeder H5A7E50 15 3
Sasha Feb 14, 2011 Derek Fry B9P6F82 16 7
Quon Aug 3, 2010 Jakeem Booth M6P5D91 13 8
Mira May 9, 2008 Erich Cummings I5B5D50 14 6
Galena Dec 20, 2009 Channing Bradley W3B9O80 18 5
Iris Mar 18, 2011 Flynn Preston Z4I0V30 13 2
Hayley Aug 31, 2011 Bruno Stone I6R3O08 12 8
Lana Jun 21, 2009 Ivan Randolph P3D7O33 14 3
Justine Aug 1, 2007 Vladimir Pickett W4V7N93 13 3
Nina Mar 3, 2010 Carlos Kennedy K7V7B68 13 4
Beverly Jan 6, 2008 Jacob Sanders U0U1E35 18 5
Kirby Mar 28, 2008 Dieter Jones F3C0P80 18 5

Melbourne 3000
Alana Aug 22, 2011 Kieran Huffman E7U6P20 18 2
Aspen Aug 3, 2009 Cyrus Anthony C8X1S92 16 5
Inez Jun 15, 2011 Davis Huff C8R1Q97 12 3
Alika Jun 8, 2009 Nissim Taylor F4X5Y04 13 3
Risa May 19, 2009 Alden Weber Y6Y6T83 17 2
Yuri Jan 3, 2008 Felix Lang N3P9M98 14 8
Imani Dec 10, 2009 Marsden Kinney C3H4D06 18 3
Emily Aug 7, 2009 Colin Mercado E7O9A19 16 5
Azalia May 30, 2010 Amery Whitley N1Z1A76 16 3
Zoe Nov 5, 2010 Jordan Olson Z5W9E49 14 2
Basia May 28, 2011 Richard Walton F8S9J25 19 5
April Sep 4, 2007 Hayden Mays A6B9Y55 19 4
Kaitlin Nov 7, 2008 Tate Landry K2U9D82 13 4
Alexis Apr 22, 2009 Chandler Kline A1C5A28 19 3

D Analysis Software Transcripts

These transcripts were made using the SCRIPT utility, standard on most unix systems. To preserve the record of each session for evidence purposes, no attempt has been made to manipulate or format these transcripts to make them more easily readable (e.g. by removing ANSI codes or extended keystrokes).

The original logs have been kept by the investigator and can be provided if required. Digests of these logs can be found in the following appendix (on page 89).

D.1 mmls and mmcat

```
Script started on Wed 13 Oct 2010 10:59:22 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mmls -
vbr disk-image.img
tsk_img_open: Type: 0 NumImg: 1 Img1: disk-image.img
Not an EWF file
dos_load_prim: Table Sector: 0
tsk_img_read: Loading data into cache 3 (0)
raw_read: byte offset: 0 len: 65536
dos_load_prim_table: Testing FAT/NTFS conditions
load_pri:0:0 Start: 20480 Size: 204800 Type: 11
load_pri:0:1 Start: 266240 Size: 204800 Type: 131
load_pri:0:2 Start: 0 Size: 0 Type: 0
load_pri:0:3 Start: 0 Size: 0 Type: 0
bsd_load_table: Table Sector: 1
tsk_img_read: Read found in cache 3
gpt_load_table: Sector: 0
tsk_img_read: Read found in cache 3
sun_load_table: Trying sector: 0
tsk_img_read: Read found in cache 3
sun_load_table: Trying sector: 1
tsk_img_read: Read found in cache 3
mac_load_table: Sector: 1
tsk_img_read: Read found in cache 3
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors
Slot Start End Length Size Description
00: Meta 0000000000 0000000000 0000000001 0512B Primary Table (#0)
01: ----- 0000000000 0000020479 0000020480 0010M Unallocated
02: 00:00 0000020480 0000225279 0000204800 0100M Win95 FAT32 (0x0B)
03: ----- 0000225280 0000266239 0000040960 0020M Unallocated
04: 00:01 0000266240 0000471039 0000204800 0100M Linux (0x83)
dos_load_prim: Table Sector: 20480
tsk_img_read: Loading data into cache 2 (10485760)
raw_read: byte offset: 10485760 len: 65536
dos_load_prim_table: Testing FAT/NTFS conditions
load_pri:0:0 Start: 0 Size: 0 Type: 0
load_pri:0:1 Start: 0 Size: 0 Type: 0
load_pri:0:2 Start: 0 Size: 0 Type: 0
load_pri:0:3 Start: 0 Size: 0 Type: 0
dos_load_prim: No valid entries
bsd_load_table: Table Sector: 20481
tsk_img_read: Read found in cache 2
gpt_load_table: Sector: 20480
tsk_img_read: Read found in cache 2
sun_load_table: Trying sector: 20480
tsk_img_read: Read found in cache 2
sun_load_table: Trying sector: 20481
tsk_img_read: Read found in cache 2
mac_load_table: Sector: 20481
tsk_img_read: Read found in cache 2
dos_load_prim: Table Sector: 266240
tsk_img_read: Loading data into cache 1 (136314880)
raw_read: byte offset: 136314880 len: 0
bsd_load_table: Table Sector: 266241
tsk_img_read: Loading data into cache 1 (136315392)
raw_read: byte offset: 136315392 len: 4294966784
gpt_load_table: Sector: 266240
tsk_img_read: Loading data into cache 1 (136314880)
raw_read: byte offset: 136314880 len: 0
```

```
sun_load_table: Trying sector: 266240
tsk_img_read: Loading data into cache 1 (136314880)
raw_read: byte offset: 136314880 len: 0
mac_load_table: Sector: 266241
tsk_img_read: Loading data into cache 1 (136315392)
raw_read: byte offset: 136315392 len: 4294966784
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mm-
cal[Kt disk-image.img 0 > disk-image.img [K[K[K[K[K[K[K[K[Kpart0.img
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mm-
cat disk-image.img 0 > disk-part0.img[1P.img1.img[1P[1@1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mm-
cat disk-image.img 1 > disk-part1.img[1P.img2.img[1P[1@2
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mm-
cat disk-image.img 2 > disk-part2.img[1P.img3.img[C[1P[1@3
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Wed 13 Oct 2010 11:00:49 EST
```

D.2 Hidden FAT16 FS Analysis

```
Script started on Wed 13 Oct 2010 16:28:30 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file disk-
part3.img
disk-part3.img: x86 boot sector, mkdosfs boot message display, code offset 0x3c, OEM-ID " mk-
dosfs", sectors/cluster 4, root entries 512, sectors 40960 (volumes <=32 MB) , Media descrip-
tor 0xf8, sectors/FAT 40, heads 64, serial number 0xeac1d612, la-
bel: "           ", FAT (16 bit)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  fls -
lr disk-part3.img
r/r 3:  REPLICA_.JPG 2012-12-12 11:12:00 (EST) 0000-00-00 00:00:00 (UTC)
0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 49304 0 0
v/v 654067:  $MBR 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC)
0000-00-00 00:00:00 (UTC) 512 0 0
v/v 654068:  $FAT1 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC)
0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 20480 0 0
v/v 654069:  $FAT2 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC)
0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 20480 0 0
d/d 654070:  $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC)
0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat disk-
part3.img 3 > REPLICA_.JPG
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum REPLICA_.JPG
21522b41731798592433357199215fda  REPLICA_.JPG
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file REPLICA_.JPG
REPLICA_.JPG: JPEG image data, JFIF standard 1.02
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -dTvao REPLICA_.JPG [K.carve REPLICA_.JPG
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Wed Oct 13 16:31:22 2010
Invocation: foremost -dTvao REPLICA_.JPG.carve REPLICA_.JPG
Output directory: /var/evidence/REPLICA_.JPG.carve_Wed_Oct_13_16_31_22_2010
Configuration file: /etc/foremost.conf
Processing: REPLICA_.JPG
|------------------------------------------------------------------
File: REPLICA_.JPG
Start: Wed Oct 13 16:31:22 2010
Length: 48 KB (49304 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
0:  00000000.jpg        45 KB           0
1:  00000064.bmp        15 KB        32938    (Header dump)
2:  00000091.rar         2 KB        46604   Password Protected:
3:  00000036.exe        29 KB        18867    (Header dump)
*|
Finish: Wed Oct 13 16:31:22 2010
4 FILES EXTRACTED
jpg:= 1
bmp:= 1
rar:= 1
exe:= 1
------------------------------------------------------------------
```

```
Foremost finished at Wed Oct 13 16:31:22 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -dTvao disk-i[Kpart3.img disk-part3.img.carve
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Wed Oct 13 16:32:15 2010
Invocation: foremost -dTvao disk-part3.img disk-part3.img.carve
Output directory: /var/evidence/disk-part3.img_Wed_Oct_13_16_32_15_2010
Configuration file: /etc/foremost.conf
Processing: disk-part3.img
|------------------------------------------------------------------
File: disk-part3.img
Start: Wed Oct 13 16:32:15 2010
Length: 20 MB (20971520 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
0:  00000117.jpg        45 KB        59904
1:  00000181.bmp         2 MB        92842    (Header dump)
2:  00000208.rar         2 KB       106508   Password Protected:
3:  00000153.exe      1024 KB        78771    (Header dump)
*|
Finish: Wed Oct 13 16:32:19 2010
4 FILES EXTRACTED
jpg:= 1
bmp:= 1
rar:= 1
exe:= 1
------------------------------------------------------------------
Foremost finished at Wed Oct 13 16:32:19 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Wed 13 Oct 2010 16:32:25 EST
Script started on Wed 13 Oct 2010 19:16:15 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ dosfsck -
nfv disk-part3.img
dosfsck 3.0.7 (24 Dec 2009)
dosfsck 3.0.7, 24 Dec 2009, FAT32, LFN
Checking we can access the last sector of the filesystem
Boot sector contents:
System ID "mkdosfs"
Media byte 0xf8 (hard disk)
       512 bytes per logical sector
      2048 bytes per cluster
         1 reserved sector
First FAT starts at byte 512 (sector 1)
         2 FATs, 16 bit entries
     20480 bytes per FAT (= 40 sectors)
Root directory starts at byte 41472 (sector 81)
       512 root directory entries
Data area starts at byte 57856 (sector 113)
     10211 data clusters (20912128 bytes)
32 sectors/track, 64 heads
         0 hidden sectors
     40960 sectors total
Reclaiming unconnected clusters.
disk-part3.img: 1 files, 25/10211 clusters
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  hd disk-
part3.img | head -35
00000000  eb 3c 90 6d 6b 64 6f 73  66 73 00 00 02 04 01 00  |.<.mkdosfs......|
00000010  02 00 02 00 a0 f8 28 00  20 00 40 00 00 00 00 00  |......(. .@.....|
00000020  00 00 00 00 00 00 29 12  d6 c1 ea 20 20 20 20 20  |......)....     |
00000030  20 20 20 20 20 20 46 41  54 31 36 20 20 20 0e 1f  |      FAT16   ..|
00000040  be 5b 7c ac 22 c0 74 0b  56 b4 0e bb 07 00 cd 10  |.[|.".t.V.......|
00000050  5e eb f0 32 e4 cd 16 cd  19 eb fe 54 68 69 73 20  |^..2.......This |
00000060  69 73 20 6e 6f 74 20 61  20 62 6f 6f 74 61 62 6c  |is not a bootabl|
00000070  65 20 64 69 73 6b 2e 20  20 50 6c 65 61 73 65 20  |e disk.  Please |
00000080  69 6e 73 65 72 74 20 61  20 62 6f 6f 74 61 62 6c  |insert a bootabl|
00000090  65 20 66 6c 6f 70 70 79  20 61 6e 64 0d 0a 70 72  |e floppy and..pr|
000000a0  65 73 73 20 61 6e 79 20  6b 65 79 20 74 6f 20 74  |ess any key to t|
000000b0  72 79 20 61 67 61 69 6e  20 2e 2e 2e 20 0d 0a 00  |ry again ... ...|
000000c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
```

```
00000200  f8 ff ff ff 00 00 04 00  05 00 06 00 07 00 08 00  |................|
00000210  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
00000220  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
00000230  19 00 1a 00 1b 00 ff ff  00 00 00 00 00 00 00 00  |................|
00000240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00005200  f8 ff ff ff 00 00 04 00  05 00 06 00 07 00 08 00  |................|
00005210  09 00 0a 00 0b 00 0c 00  0d 00 0e 00 0f 00 10 00  |................|
00005220  11 00 12 00 13 00 14 00  15 00 16 00 17 00 18 00  |................|
00005230  19 00 1a 00 1b 00 ff ff  00 00 00 00 00 00 00 00  |................|
00005240  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
0000a200  52 45 50 4c 49 43 41 5f  4a 50 47 20 00 00 00 00  |REPLICA_JPG ....|
0000a210  00 00 00 00 00 00 80 59  8c 41 03 00 98 c0 00 00  |.......Y.A......|
0000a220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
0000ea00  ff d8 ff e0 00 10 4a 46  49 46 00 01 02 00 00 64  |......JFIF.....d|
0000ea10  00 64 00 00 ff ec 00 11  44 75 63 6b 79 00 01 00  |.d......Ducky...|
0000ea20  04 00 00 00 1e 00 00 ff  ee 00 0e 41 64 6f 62 65  |...........Adobe|
0000ea30  00 64 c0 00 00 00 01 ff  db 00 84 00 10 0b 0b 0b  |.d..............|
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ hd disk-
part3.img | tail
0001aa30  44 91 b5 5d 7c eb 7b e9  39 b0 45 63 3e a3 e5 cf  |D..]|.{.9.Ec>...|
0001aa40  50 af a8 4c 70 ce 32 f3  bf ed f8 c1 d8 b4 89 6b  |P..Lp.2........k|
0001aa50  59 4c bc a3 ca 42 42 9b  1f 89 c9 34 9b e8 54 d7  |YL...BB....4..T.|
0001aa60  af f8 6a ea 1c fb 8e e2  bd e2 cb b7 29 7d c6 01  |..j.........)}..|
0001aa70  7b 7d 1d 4b 6e 0f 5b a9  a2 3a b7 13 b4 a8 b7 6a  |{}.Kn.[..:.....j|
0001aa80  fe f8 df f9 b5 3d 7e 21  c5 dd 55 1f 72 ac a7 1a  |.....=~!..U.r...|
0001aa90  5e c4 3d 7b 00 40 07 00  00 00 00 00 00 00 00 00  |^.={.@..........|
0001aaa0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
01400000
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  hd REPLICA_.JPG | tail -
n 8
0000c030  44 91 b5 5d 7c eb 7b e9  39 b0 45 63 3e a3 e5 cf  |D..]|.{.9.Ec>...|
0000c040  50 af a8 4c 70 ce 32 f3  bf ed f8 c1 d8 b4 89 6b  |P..Lp.2........k|
0000c050  59 4c bc a3 ca 42 42 9b  1f 89 c9 34 9b e8 54 d7  |YL...BB....4..T.|
0000c060  af f8 6a ea 1c fb 8e e2  bd e2 cb b7 29 7d c6 01  |..j.........)}..|
0000c070  7b 7d 1d 4b 6e 0f 5b a9  a2 3a b7 13 b4 a8 b7 6a  |{}.Kn.[..:.....j|
0000c080  fe f8 df f9 b5 3d 7e 21  c5 dd 55 1f 72 ac a7 1a  |.....=~!..U.r...|
0000c090  5e c4 3d 7b 00 40 07 00                           |^.={.@..|
0000c098
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Wed 13 Oct 2010 19:19:46 EST
Script started on Wed 13 Oct 2010 19:40:01 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum REPLICA_.JPG
21522b41731798592433357199215fda  REPLICA_.JPG
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  md5sum REPLICA_.JPG.carve_Wed_O
part3.img_Wed_Oct_13_16_32_15_2010/jpg/00000117.jpg
67df476a6524a57953204dcf82a80a23  REPLICA_.JPG.carve_Wed_Oct_13_16_31_22_2010/jpg/00000000.jpg
67df476a6524a57953204dcf82a80a23  disk-part3.img_Wed_Oct_13_16_32_15_2010/jpg/00000117.jpg
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum REPLICA_.JPG.carve_Wed_Oc
part3.img_Wed_Oct_13_16_32_15_2010/rar/00000208.rar
763da572e4cf48f699d708611c1b0bab  REPLICA_.JPG.carve_Wed_Oct_13_16_31_22_2010/rar/00000091.rar
763da572e4cf48f699d708611c1b0bab  disk-part3.img_Wed_Oct_13_16_32_15_2010/rar/00000208.rar
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Wed 13 Oct 2010 19:40:45 EST
```

D.3 RAR File Decryption

```
Script started on Wed 13 Oct 2010 23:28:53 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%
Encrypted file:  CRC failed in Local.txt (password incorrect ?)
Total errors: 1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
```

```
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%
Encrypted file:  CRC failed in Local.txt (password incorrect ?)
Total errors: 1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%
Encrypted file:  CRC failed in Local.txt (password incorrect ?)
Total errors: 1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%
Encrypted file:  CRC failed in Local.txt (password incorrect ?)
Total errors: 1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%
Encrypted file:  CRC failed in Local.txt (password incorrect ?)
Total errors: 1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar x 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Extracting from 00000091.rar
Enter password (will not be echoed) for Local.txt:
Extracting  Local.txt                                                 97%  OK
All OK
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum Lo-
cal.txt
f5c51891b5506edbf8cbb60798cb7d6f  Local.txt
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ head l[KLocal.txt
Fitzroy North 3068
Azalia Apr 3, 2010 Russell Hartman E9W5X31 12 7
Idola Jun 6, 2011 Caesar Boyd R6R0H01 14 3
Rhona Oct 3, 2008 Burke Fitzgerald H0P4E86 15 7
Lacy Sep 6, 2009 Conan Ward O5A7X51 19 8
Darrel Dec 28, 2007 Keith Decker R7D2F67 15 6
MacKensie Jan 18, 2010 Allistair Moran H9E4W37 13 5
Carissa Jun 5, 2008 Lance Cobb L8U1F24 19 3
Cleo Nov 30, 2010 Tyrone Goodman Q7R3Z86 18 3
Vivien Sep 15, 2009 Xenos Solomon C2D5C44 17 5
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ tail Lo-
cal.txt
Risa May 19, 2009 Alden Weber Y6Y6T83 17 2
Yuri Jan 3, 2008 Felix Lang N3P9M98 14 8
Imani Dec 10, 2009 Marsden Kinney C3H4D06 18 3
Emily Aug 7, 2009 Colin Mercado E7O9A19 16 5
Azalia May 30, 2010 Amery Whitley N1Z1A76 16 3
Zoe Nov 5, 2010 Jordan Olson Z5W9E49 14 2
Basia May 28, 2011 Richard Walton F8S9J25 19 5
April Sep 4, 2007 Hayden Mays A6B9Y55 19 4
Kaitlin Nov 7, 2008 Tate Landry K2U9D82 13 4
Alexis Apr 22, 2009 Chandler Kline A1C5A28 19 3
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ wc Lo-
cal.txt
 116  911 4697 Local.txt
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Wed 13 Oct 2010 23:32:25 EST
```

D.4 Initial File Analysis

```
Script started on Thu 14 Oct 2010 10:54:57 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  fls -
r disk-part2.img | head
d/d 4:  John S
+ d/d 22:  Recent
++ r/r 40:  replica_state_license_plate.gif.lnk
++ r/r 42:  Desktop.ini
++ r/r 44:  Links.txt.lnk
++ r/r 50:  transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2).lnk
+ r/r 24:  ntuser.ini
+ d/d 26:  My Documents
++ d/d 150:  My Music
+++ r/r 167:  Sample Music.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat disk-
part2.img 40 > replica_state_license_plate.gif.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum replica_state_license_pla
e3f451501f42e1f130ca93241974e713  replica_state_license_plate.gif.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep -i local.txt
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep -i local.txt[K[K[K[K[K[K[K[K[Kstate_licence[K[Kse
++ r/r 40:  replica_state_license_plate.gif.lnk
++ r/r 154:  replica_state_license_plate.gif
++ r/r 2188:
http--headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url
++ r/r * 6205:  replica_state_license_plate.gif
+++++ r/r 616545:  replica_state_license_plate[1].gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat disk-
part2.img 154 > replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat disk-
part2.img 2188:[K > http--headsteadi.com-wp-content-uploads-2008-04 -
replica_state_license_plate.gif.url
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file *replica_state_license_plat
http--headsteadi.com-wp-content-uploads-2008-04-
replica_state_license_plate.gif.url: ASCII text, with CRLF line terminators
replica_state_license_plate.gif:                                          GIF im-
age data, version 87a, 500 x 335
replica_state_license_plate.gif.lnk:                                      MS Win-
dows shortcut
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum  *replica_state_license_pl
ece7a04cfe3b5659471ad230958b7cc2  http--headsteadi.com-wp-content-uploads-2008-04-
replica_state_license_plate.gif.url
afb056f39ef61a1d208c08afa4c6adba  replica_state_license_plate.gif
e3f451501f42e1f130ca93241974e713  replica_state_license_plate.gif.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 11:09:39 EST
Script started on Thu 14 Oct 2010 11:15:56 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep -i links.txt
++ r/r 44:  Links.txt.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep -i -C 5 Recent
d/d 4:  John S
+ d/d 22:  Recent
++ r/r 40:  replica_state_license_plate.gif.lnk
++ r/r 42:  Desktop.ini
++ r/r 44:  Links.txt.lnk
++ r/r 50:  transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2).lnk
+ r/r 24:  ntuser.ini
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat 44 [K[K[Kdisk-
part2.img 44 > Links.txt.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum Links.txt.lnk
a8df937402dfce8575fe73041edd9a58  Links.txt.lnk
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file Links.txt.lnk
Links.txt.lnk: MS Windows shortcut
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 11:18:52 EST
```

D.5 replica_state_license_plate.gif and related files

```
Script started on Thu 14 Oct 2010 21:11:34 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  fore-
most -wd replica_state_license_plate.gif
Processing: replica_state_license_plate.gif
|*|
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cat out-
put/audit.txt
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Thu Oct 14 21:11:49 2010
Invocation: foremost -wd replica_state_license_plate.gif
Output directory: /var/evidence/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: replica_state_license_plate.gif
Start: Thu Oct 14 21:11:49 2010
Length: 56 KB (57632 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
0:           0.(null)          gif   3213033948   (null)
Finish: Thu Oct 14 21:11:49 2010
1 FILES EXTRACTED
gif:= 1
------------------------------------------------------------------
Foremost finished at Thu Oct 14 21:11:49 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  hd http-
-headsteadi.com-wp-content-uploads-2008-04-replica_state_license_ plate.gif.url
00000000  5b 44 45 46 41 55 4c 54  5d 0d 0a 42 41 53 45 55  |[DEFAULT]..BASEU|
00000010  52 4c 3d 68 74 74 70 3a  2f 2f 68 65 61 64 73 74  |RL=http://headst|
00000020  65 61 64 69 2e 63 6f 6d  2f 77 70 2d 63 6f 6e 74  |eadi.com/wp-cont|
00000030  65 6e 74 2f 75 70 6c 6f  61 64 73 2f 32 30 30 38  |ent/uploads/2008|
00000040  2f 30 34 2f 72 65 70 6c  69 63 61 5f 73 74 61 74  |/04/replica_stat|
00000050  65 5f 6c 69 63 65 6e 73  65 5f 70 6c 61 74 65 2e  |e_license_plate.|
00000060  67 69 66 0d 0a 5b 49 6e  74 65 72 6e 65 74 53 68  |gif..[InternetSh|
00000070  6f 72 74 63 75 74 5d 0d  0a 55 52 4c 3d 68 74 74  |ortcut]..URL=htt|
00000080  70 3a 2f 2f 68 65 61 64  73 74 65 61 64 69 2e 63  |p://headsteadi.c|
00000090  6f 6d 2f 77 70 2d 63 6f  6e 74 65 6e 74 2f 75 70  |om/wp-content/up|
000000a0  6c 6f 61 64 73 2f 32 30  30 38 2f 30 34 2f 72 65  |loads/2008/04/re|
000000b0  70 6c 69 63 61 5f 73 74  61 74 65 5f 6c 69 63 65  |plica_state_lice|
000000c0  6e 73 65 5f 70 6c 61 74  65 2e 67 69 66 0d 0a 4d  |nse_plate.gif..M|
000000d0  6f 64 69 66 69 65 64 3d  42 30 36 45 34 39 38 30  |odified=B06E4980|
000000e0  31 31 34 44 43 42 30 31  31 31 0d 0a 49 63 6f 6e  |114DCB0111..Icon|
000000f0  46 69 6c 65 3d 68 74 74  70 3a 2f 2f 68 65 61 64  |File=http://head|
00000100  73 74 65 61 64 69 2e 63  6f 6d 2f 66 61 76 69 63  |steadi.com/favic|
00000110  6f 6e 2e 69 63 6f 0d 0a  49 63 6f 6e 49 6e 64 65  |on.ico..IconInde|
00000120  78 3d 31 0d 0a                                    |x=1..|
00000125
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cat http-
-headsteadi.com-wp-content-uploads-2008-04-replica_state_license_ plate.gif.url
[DEFAULT]
BASEURL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
[InternetShortcut]
URL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
Modified=B06E4980114DCB0111
IconFile=http://headsteadi.com/favicon.ico
IconIndex=1
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
lr disk-part2.img | head -3
d/d 4:  John S  2012-12-12 11:12:00 (EST)       2012-12-12 00:00:00 (EST)       0000-00-
00 00:00:00 (UTC)2010-09-08 16:06:56 (EST) 1536    0       0
+ d/d 22:       Recent  2012-12-12 11:12:00 (EST)       2012-12-12 00:00:00 (EST)       0000-
00-00 00:00:00 (UTC)        2010-09-08 16:06:56 (EST)       512     0       0
++ r/r 40:      replica_state_license_plate.gif.lnk     2012-12-12 11:12:00 (EST)       2012-
12-12 00:00:00 (EST)        0000-00-00 00:00:00 (UTC)       2010-09-
08 16:06:56 (EST)       503     0       0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ hd replica_state_license_plate.g
00000000  4c 00 00 00 01 14 02 00  00 00 00 00 c0 00 00 00  |L...............|
00000010  00 00 00 46 9b 00 00 00  20 00 00 00 60 b7 33 98  |...F.... ...‘.3.|
00000020  11 4d cb 01 00 f0 33 a1  02 4d cb 01 00 fd f1 62  |.M....3..M.....b|
00000030  11 4d cb 01 20 e1 00 00  00 00 00 00 01 00 00 00  |.M.. ...........|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 86 00 84 00  |................|
00000050  32 00 00 00 00 00 00 00  00 00 00 00 72 65 70 6c  |2...........repl|
```

```
00000060  69 63 61 5f 73 74 61 74  65 5f 6c 69 63 65 6e 73  |ica_state_licens|
00000070  65 5f 70 6c 61 74 65 2e  67 69 66 00 56 00 03 00  |e_plate.gif.V...|
00000080  04 00 ef be 00 00 00 00  00 00 00 00 14 00 00 00  |................|
00000090  72 00 65 00 70 00 6c 00  69 00 63 00 61 00 5f 00  |r.e.p.l.i.c.a._.|
000000a0  73 00 74 00 61 00 74 00  65 00 5f 00 6c 00 69 00  |s.t.a.t.e._.l.i.|
000000b0  63 00 65 00 6e 00 73 00  65 00 5f 00 70 00 6c 00  |c.e.n.s.e._.p.l.|
000000c0  61 00 74 00 65 00 2e 00  67 00 69 00 66 00 00 00  |a.t.e...g.i.f...|
000000d0  2e 00 00 00 77 00 00 00  1c 00 00 00 01 00 00 00  |....w...........|
000000e0  1c 00 00 00 2d 00 00 00  00 00 00 00 76 00 00 00  |....-.......v...|
000000f0  11 00 00 00 03 00 00 00  9e 3d 9a 70 10 00 00 00  |.........=.p....|
00000100  00 43 3a 5c 44 6f 63 75  6d 65 6e 74 73 20 61 6e  |.C:\Documents an|
00000110  64 20 53 65 74 74 69 6e  67 73 5c 4a 6f 68 6e 20  |d Settings\John |
00000120  53 5c 44 65 73 6b 74 6f  70 5c 72 65 70 6c 69 63  |S\Desktop\replic|
00000130  61 5f 73 74 61 74 65 5f  6c 69 63 65 6e 73 65 5f  |a_state_license_|
00000140  70 6c 61 74 65 2e 67 69  66 00 00 2a 00 2e 00 2e  |plate.gif..*....|
00000150  00 5c 00 44 00 65 00 73  00 6b 00 74 00 6f 00 70  |.\.D.e.s.k.t.o.p|
00000160  00 5c 00 72 00 65 00 70  00 6c 00 69 00 63 00 61  |.\.r.e.p.l.i.c.a|
00000170  00 5f 00 73 00 74 00 61  00 74 00 65 00 5f 00 6c  |._.s.t.a.t.e._.l|
00000180  00 69 00 63 00 65 00 6e  00 73 00 65 00 5f 00 70  |.i.c.e.n.s.e._.p|
00000190  00 6c 00 61 00 74 00 65  00 2e 00 67 00 69 00 66  |.l.a.t.e...g.i.f|
000001a0  00 28 00 43 00 3a 00 5c  00 44 00 6f 00 63 00 75  |.(.C.:.\.D.o.c.u|
000001b0  00 6d 00 65 00 6e 00 74  00 73 00 20 00 61 00 6e  |.m.e.n.t.s. .a.n|
000001c0  00 64 00 20 00 53 00 65  00 74 00 74 00 69 00 6e  |.d. .S.e.t.t.i.n|
000001d0  00 67 00 73 00 5c 00 4a  00 6f 00 68 00 6e 00 20  |.g.s.\.J.o.h.n. |
000001e0  00 53 00 5c 00 44 00 65  00 73 00 6b 00 74 00 6f  |.S.\.D.e.s.k.t.o|
000001f0  00 70 00 00 00 00 00                              |.p.....|
000001f7
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 21:12:31 EST
Script started on Thu 14 Oct 2010 21:36:33 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ grep URL http-
-headsteadi.com-wp-content-uploads-2008-04-replica_state_lic ense_plate.gif.url
BASEURL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
URL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ wget -
O rslb.gif --quiet http://headsteadi.com/wp-
content/uploads/2008/04/ replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum rslb.gif replica_state_li
afb056f39ef61a1d208c08afa4c6adba  rslb.gif
afb056f39ef61a1d208c08afa4c6adba  replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ diff  rslb.gif replica_state_lic
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 21:37:49 EST
```

D.6 Initial partition.img analysis

```
Script started on Fri 15 Oct 2010 00:34:23 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rl disk-part2.img > disk-part2.ls
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rl partition.img > partition.ls
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ diff *.ls
8c8
< + d/d 26:  My Documents 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 512 0 0
---
> + d/d 26:  My Documents 2010-09-12 12:44:34 (EST) 2010-09-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 512 0 0
12c12
< ++ r/r 154:  replica_state_license_plate.gif 2012-12-12 11:12:00 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 57632 0 0
---
> ++ r/r * 154:  replica_state_license_plate.gif 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 57856 0 0
16a17
> ++ r/r * 162:  I9qQ5WEYf5oAV-77roMCcmqQt403aRa 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 0 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  diff -
u *.ls
--- disk-part2.ls 2010-10-15 00:34:33.000000000 +1100
```

```
+++ partition.ls 2010-10-15 00:34:38.000000000 +1100
@@ -5,15 +5,16 @@
 ++ r/r 44:  Links.txt.lnk 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 530 0 0
 ++ r/r 50:  transfer on rohit-laptop server (Samba, Ubuntu) (10.0.0.2).lnk
2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC)
2010-09-08 16:06:56 (EST) 493 0 0
 + r/r 24:  ntuser.ini 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 178 0 0
-+ d/d 26:  My Documents 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 512 0 0
++ d/d 26:  My Documents 2010-09-12 12:44:34 (EST) 2010-09-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 512 0 0
 ++ d/d 150:  My Music 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 512 0 0
 +++ r/r 167:  Sample Music.lnk 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 542 0 0
 +++ r/r 169:  Desktop.ini 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 182 0 0
-++ r/r 154:  replica_state_license_plate.gif 2012-12-12 11:12:00 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 57632 0 0
+++ r/r * 154:  replica_state_license_plate.gif 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 57856 0 0
 ++ r/r 156:  desktop.ini 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 77 0 0
 ++ d/d 158:  My Pictures 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 512 0 0
 +++ r/r 2055:  Sample Pictures.lnk 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 572 0 0
 +++ r/r 2057:  Desktop.ini 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 184 0 0
+++ r/r * 162:  I9qQ5WEYf5oAV-77roMCcmqQt403aRa 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 0 0 0
 + d/d 28:  SendTo 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 1024 0 0
 ++ r/r 2121:  Compressed (zipped) Folder.ZFSendToTarget 2012-12-12 11:12:00 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 0 0 0
 ++ r/r 2124:  My Documents.mydocs 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 0 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Fri 15 Oct 2010 00:34:50 EST
```

D.7 Registry analysis

```
Script started on Thu 14 Oct 2010 21:47:14 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  fls -
lr disk-part2.img | grep NTUSER
+ r/r 2459:  NTUSER.DAT.LOG 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 1024 0 0
+ r/r 2460:  NTUSER.DAT 2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST)
0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 786432 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat disk-
part2.img 2460 > NTUSER.DAT
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum NTUSER.DAT
015eead6ba2872e9eaebdbf160cd045e  NTUSER.DAT
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file NTUSER.DAT
NTUSER.DAT: MS Windows registry file, NT/2000 or above
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT | head
PATH,TYPE,VALUE,MTIME
/,KEY■2010-09-05 15:26:16
/AppEvents,KEY■2010-09-05 15:02:42
/AppEvents/EventLabels,KEY■2010-09-05 15:02:48
/AppEvents/EventLabels/.Default,KEY■2010-09-05 15:02:42
/AppEvents/EventLabels/.Default/,SZ,Default Beep,
/AppEvents/EventLabels/.Default/DispFileName,SZ,@mmsys.cpl\x2C-5824,
/AppEvents/EventLabels/ActivatingDocument,KEY■2010-09-05 15:02:45
/AppEvents/EventLabels/ActivatingDocument/,SZ,Complete Navigation,
/AppEvents/EventLabels/AppGPFault,KEY■2010-09-05 15:02:42
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ reglookup-
timeline NTUSER.DAT  | head
```

```
MTIME,FILE,PATH
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/AppGPFault
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/Close
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/CriticalBatteryAlarm
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/.Default
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceConnect
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceDisconnect
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceFail
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/EmptyRecycleBin
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ reglookup-
recover NTUSER.DAT
OFFSET,REC_LENGTH,REC_TYPE,PATH,NAME,NK_MTIME,NK_NVAL,VK_TYPE,VK_VALUE,VK_DATA_LEN,SK_OWNER,SK_GROUP,SK_SACL,SK_DACL,R
0006F080,00000030,VALUE■UserRequestedUpdate■,DWORD,0x00000000,4■■,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT | grep replica_state
/Software/Microsoft/Internet Explorer/TypedURLs/url3,SZ,http://headsteadi.com/wp-
content/uploads/2008/04/replica_state_license_plate.gif,
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/*/b,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CMy Documents\x5Creplica_state_license_plate.gif,
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/*/c,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CDesktop\x5Creplica_state_license_plate.gif,
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/gif/a,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CMy Documents\x5Creplica_state_license_plate.gif,
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/gif/b,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CDesktop\x5Creplica_state_license_plate.gif,
/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs/2,BINARY,r\x00e\x00p\x00l\x00i\x00c\x00a\x00_\x00s\x00t
/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs/.gif/0,BINARY,r\x00e\x00p\x00l\x00i\x00c\x00a\x00_\x00s
/Software/Microsoft/Windows/CurrentVersion/Webcheck/Store.1/{8021D69B-4D11-01CB-0000-
0000701F3784}/,SZ,http--headsteadi.com-wp-content-uploads-2008-04-
replica_state_license_plate.gif,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  re-
glookup NTUSER.DAT | grep Links.txt
/Software/Microsoft/Windows/CurrentVersion/Applets/Wordpad/Recent File List/File1,SZ,\x5C\x5C10.0.0.2\x5Ctransfer\x5CL
/Software/Microsoft/Windows/CurrentVersion/Explorer/RecentDocs/.txt/0,BINARY,L\x00i\x00n\x00k\x00s\x00.\x00t\x00x\x00t
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT | grep tandi
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/*/a,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CDesktop\x5C{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf,
/Software/Microsoft/Windows/CurrentVersion/Explorer/ComDlg32/OpenSaveMRU/pdf/a,SZ,C:\x5CDocuments and Set-
tings\x5CJohn S\x5CDesktop\x5C{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT | grep -i Local.txt
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 21:55:00 EST
Script started on Thu 14 Oct 2010 22:24:26 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT | grep -i rar
/Software/Microsoft/Windows/CurrentVersion/Explorer/Shell Fold-
ers/Cache,SZ,C:\x5CDocuments and Settings\x5CJohn S\x5CLocal Settings\x5CTemporary Inter-
net Files,
/Software/Microsoft/Windows/CurrentVersion/Explorer/User Shell Fold-
ers/Cache,EXPAND_SZ,%USERPROFILE%\x5CLocal Settings\x5CTemporary Internet Files,
/Software/Microsoft/Windows/ShellNoRoam/MUICache/@C:\x5CWINDOWS\x5Cinf\x5Cunregmp2.exe\x2C-
9924,SZ,Windows Media Library,
/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/ExcludeProfileDirs,SZ,Local Set-
tings;Temporary Internet Files;History;Temp,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ reglookup-
timeline NTUSER.DAT | head
MTIME,FILE,PATH
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/AppGPFault
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/Close
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/CriticalBatteryAlarm
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/.Default
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceConnect
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceDisconnect
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/DeviceFail
2010-09-05 15:02:42,NTUSER.DAT,/AppEvents/EventLabels/EmptyRecycleBin
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ reglookup-
timeline NTUSER.DAT | tail
2010-09-
```

```
05 15:49:34,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/Explorer/UserAssist/{5E6AB780-
7743-11CF-A12B-00AA004AE837}/Count
2010-09-05 15:49:43,NTUSER.DAT,/Software/Microsoft/Windows/Shell/Bags/2/Shell
2010-09-05 15:49:54,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/Explorer/StuckRects2
2010-09-05 15:49:58,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion
2010-09-05 15:50:02,NTUSER.DAT,/Software/Microsoft/CTF/MSUTB
2010-09-05 15:50:02,NTUSER.DAT,/Software/Microsoft/Internet Explorer/Desktop/Old WorkAreas
2010-09-05 15:50:02,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/Explorer
2010-09-05 15:50:02,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/Explorer/StartPage
2010-09-05 15:50:02,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/Explorer/TrayNotify
2010-09-05 15:50:05,NTUSER.DAT,/Software/Microsoft/Windows/CurrentVersion/WindowsUpdate
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT  | grep -i computername
/Software/Microsoft/Windows Media/WMSDK/General/ComputerName,SZ,JOHNS-93885B985,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT  | grep -i username
/Identities/Last Username,SZ,Main Identity,
/Identities/{1C6ACBAE-598A-4AC1-BCDE-428401EAC0B2}/Username,SZ,Main Identity,
/Software/Microsoft/Active Setup/Installed Components/{44BBA840-CC51-11CF-AAFA-
00AA00B6015C}/Username,SZ,John S,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ re-
glookup NTUSER.DAT  | grep -i identity
/Identities/Identity Ordinal,DWORD,0x00000001,
/Identities/Last Username,SZ,Main Identity,
/Identities/Identity Login,DWORD,0x00098053,
/Identities/{1C6ACBAE-598A-4AC1-BCDE-428401EAC0B2}/Username,SZ,Main Identity,
/Software/Microsoft/Protected Storage System Provider/S-1-5-21-1547161642-1383384898-
1708537768-1003/Data/89c39569-6841-11d2-9f59-0000f8085266/Display String,SZ,IdentityMgr,
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 22:24:51 EST
```

D.8 Malware

```
Script started on Thu 14 Oct 2010 23:00:53 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo mount -
o ro,loop disk-part2.img /mnt
[sudo] password for dleigh:
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo fresh-
clam
ClamAV update process started at Thu Oct 14 23:01:07 2010
main.cld is up to date (version: 52, sigs: 704727, f-level: 44, builder: sven)
daily.cld is up to date (version: 12136, sigs: 139819, f-level: 53, builder: guitar)
bytecode.cvd is up to date (version: 80, sigs: 10, f-level: 53, builder: edwin)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo clam-
scan -ri /mnt/
----------- SCAN SUMMARY -----------
Known viruses: 843322
Engine version: 0.96.3
Scanned directories: 68
Scanned files: 1848
Infected files: 0
Data scanned: 32.60 MB
Data read: 25.17 MB (ratio 1.30:1)
Time: 23.479 sec (0 m 23 s)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 23:02:39 EST
Script started on Thu 14 Oct 2010 23:04:07 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo mount -
o ro,loop disk-part3.img /mnt/
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo fresh-
clam
ClamAV update process started at Thu Oct 14 23:04:19 2010
main.cld is up to date (version: 52, sigs: 704727, f-level: 44, builder: sven)
daily.cld is up to date (version: 12136, sigs: 139819, f-level: 53, builder: guitar)
bytecode.cvd is up to date (version: 80, sigs: 10, f-level: 53, builder: edwin)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo clam-
scan -ri /mnt/
----------- SCAN SUMMARY -----------
Known viruses: 843322
Engine version: 0.96.3
```

```
Scanned directories: 1
Scanned files: 1
Infected files: 0
Data scanned: 0.05 MB
Data read: 0.05 MB (ratio 1.00:1)
Time: 10.092 sec (0 m 10 s)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ umount /mnt
umount: /mnt is not in the fstab (and you are not root)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo umount /mnt/
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Thu 14 Oct 2010 23:05:16 EST
```

D.9 Deleted Files

```
Script started on Fri 15 Oct 2010 00:27:17 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rd disk-part2.img
r/r * 6201:  John S/Desktop/{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf
r/r * 6205:  John S/Desktop/replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat disk-part2.img 6201
Directory Entry: 6201
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _7BA2B~1.PDF
Directory Entry Times:
Written:  Wed Sep  8 15:17:22 2010
Accessed:  Wed Sep  8 00:00:00 2010
Created:  Wed Sep  8 15:17:22 2010
Sectors:
4756
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat disk-part2.img 6205
Directory Entry: 6205
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _EPLIC~1.GIF
Directory Entry Times:
Written:  Wed Sep  8 15:17:22 2010
Accessed:  Wed Sep  8 00:00:00 2010
Created:  Wed Sep  8 15:17:22 2010
Sectors:
4756
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ ils disk-
part2.img
class|host|device|start_time
ils|alphonse||1287062854
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
6201|f|0|0|1283923042|1283868000|0|1283923042|777|0|0
6205|f|0|0|1283923042|1283868000|0|1283923042|777|0|0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ ils -
p disk-part2.img
class|host|device|start_time
ils|alphonse||1287062857
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ blk-
stat disk-part2.img 4756
Sector: 4756
Allocated (Meta)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Fri 15 Oct 2010 00:28:22 EST
```

D.9.1 Deleted files from partition.img

```
Script started on Fri 15 Oct 2010 11:06:16 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rld partition.img
```

```
r/r * 154:  John S/My Documents/replica_state_license_plate.gif 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 57856 0 0
r/r * 162:  John S/My Documents/I9qQ5WEYf5oAV-77roMCcmqQt403aRa 2010-09-12 12:44:34 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-12 12:44:34 (EST) 0 0 0
r/r * 6201:  John S/Desktop/{7BA2B075-9282-4331-98A6-14080E701B2B}tandi338.pdf
2010-09-08 15:17:22 (EST) 2010-09-08 00:00:00 (EST) 0000-00-00 00:00:00 (UTC)
2010-09-08 15:17:22 (EST) 0 0 0
r/r * 6205:  John S/Desktop/replica_state_license_plate.gif 2010-09-08 15:17:22 (EST)
2010-09-08 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 15:17:22 (EST) 0 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat partition.img 6205
Directory Entry: 6205
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _EPLIC~1.GIF
Directory Entry Times:
Written:  Wed Sep  8 15:17:22 2010
Accessed:  Wed Sep  8 00:00:00 2010
Created:  Wed Sep  8 15:17:22 2010
Sectors:
4756
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat partition.img 6201
Directory Entry: 6201
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _7BA2B~1.PDF
Directory Entry Times:
Written:  Wed Sep  8 15:17:22 2010
Accessed:  Wed Sep  8 00:00:00 2010
Created:  Wed Sep  8 15:17:22 2010
Sectors:
4756
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat partition.img 154
Directory Entry: 154
Not Allocated
File Attributes: File, Archive
Size: 57856
Name: _EPLIC~1.GIF
Directory Entry Times:
Written:  Sun Sep 12 12:44:34 2010
Accessed:  Wed Dec 12 00:00:00 2012
Created:  Sun Sep 12 12:44:34 2010
Sectors:
4772 4773 4774 4775 4776 4777 4778 4779
4780 4781 4782 4783 4784 4785 4786 4787
4788 4789 4790 4791 4792 4793 4794 4795
4796 4797 4798 4799 4800 4801 4802 4803
4804 4805 4806 4807 4808 4809 4810 4811
4812 4813 4814 4815 4816 4817 4818 4819
4820 4821 4822 4823 4824 4825 4826 4827
4828 4829 4830 4831 4832 4833 4834 4835
4836 4837 4838 4839 4840 4841 4842 4843
4844 4845 4846 4847 4848 4849 4850 4851
4852 4853 4854 4855 4856 4857 4858 4859
4860 4861 4862 4863 4864 4865 4866 4867
4868 4869 4870 4871 4872 4873 4874 4875
4876 4877 4878 4879 4880 4881 4882 4883
4884
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat partition.img 162
Directory Entry: 162
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _9QQ5W~1
Directory Entry Times:
Written:  Sun Sep 12 12:44:34 2010
Accessed:  Wed Dec 12 00:00:00 2012
Created:  Sun Sep 12 12:44:34 2010
```

```
Sectors:
4756
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ ils par-
tition.img
class|host|device|start_time
ils|alphonse||1287101531
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
154|f|0|0|1284259474|1355230800|0|1284259474|777|0|57856
162|f|0|0|1284259474|1355230800|0|1284259474|777|0|0
6201|f|0|0|1283923042|1283868000|0|1283923042|777|0|0
6205|f|0|0|1283923042|1283868000|0|1283923042|777|0|0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ ils -
p partition.img
class|host|device|start_time
ils|alphonse||1287101534
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat -
r partition.img 154 > replica_state_license_plate.gif.from-partition .img
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ icat -
rs partition.img 154 > replica_state_license_plate.gif.from-partitio n.img.withslack
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ md5sum replica_state_license_pla
partition.img* replica_state_l icense_plate.gif
fe3ccd72644afd348936cd7e67c0483a  replica_state_license_plate.gif.from-partition.img
fe3ccd72644afd348936cd7e67c0483a  replica_state_license_plate.gif.from-partition.img.withslack
afb056f39ef61a1d208c08afa4c6adba  replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ diff replica_state_license_plate
partition.img replica_state_lice nse_plate.gif.from-partition.img.withslack
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ file replica_state_license_plate
partition.img*
replica_state_license_plate.gif.from-partition.img:           Non-ISO extended-
ASCII text, with very long lines, with no line terminators
replica_state_license_plate.gif.from-partition.img.withslack: Non-ISO extended-
ASCII text, with very long lines, with no line terminators
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ hd replica_state_license_plate.g
partition.img | head
00000000  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
00000010  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
00000020  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
00000030  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
00000040  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
00000050  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
00000060  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
00000070  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
00000080  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
00000090  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ hd replica_state_license_plate.g
partition.img | tail
0000e170  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
0000e180  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
0000e190  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
0000e1a0  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
0000e1b0  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
0000e1c0  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
0000e1d0  92 49 24 92 49 24 92 49  24 92 49 24 92 49 24 92  |.I$.I$.I$.I$.I$.|
0000e1e0  49 24 92 49 24 92 49 24  92 49 24 92 49 24 92 49  |I$.I$.I$.I$.I$.I|
0000e1f0  24 92 49 24 92 49 24 92  49 24 92 49 24 92 49 24  |$.I$.I$.I$.I$.I$|
0000e200
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep replica_state_license_plate.gif
++ r/r 40:  replica_state_license_plate.gif.lnk
++ r/r 154:  replica_state_license_plate.gif
++ r/r 2188:
http--headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url
++ r/r * 6205:  replica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
r disk-part2.img | grep replica_state_license_plate.gif[C[C[C[C[C[C[C[1@l
++ r/r 40:  replica_state_license_plate.gif.lnk 2012-12-12 11:12:00 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 503 0 0
++ r/r 154:  replica_state_license_plate.gif 2012-12-12 11:12:00 (EST)
2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 16:06:56 (EST) 57632 0 0
++ r/r 2188:
http--headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url
2012-12-12 11:12:00 (EST) 2012-12-12 00:00:00 (EST) 0000-00-00 00:00:00 (UTC)
```

```
2010-09-08 16:06:56 (EST) 293 0 0
++ r/r * 6205:  replica_state_license_plate.gif 2010-09-08 15:17:22 (EST)
2010-09-08 00:00:00 (EST) 0000-00-00 00:00:00 (UTC) 2010-09-08 15:17:22 (EST) 0 0 0
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat disk-part2.img 154
Directory Entry: 154
Allocated
File Attributes: File, Archive
Size: 57632
Name: REPLIC~1.GIF
Directory Entry Times:
Written:  Wed Dec 12 11:12:00 2012
Accessed:  Wed Dec 12 00:00:00 2012
Created:  Wed Sep  8 16:06:56 2010
Sectors:
4772 4773 4774 4775 4776 4777 4778 4779
4780 4781 4782 4783 4784 4785 4786 4787
4788 4789 4790 4791 4792 4793 4794 4795
4796 4797 4798 4799 4800 4801 4802 4803
4804 4805 4806 4807 4808 4809 4810 4811
4812 4813 4814 4815 4816 4817 4818 4819
4820 4821 4822 4823 4824 4825 4826 4827
4828 4829 4830 4831 4832 4833 4834 4835
4836 4837 4838 4839 4840 4841 4842 4843
4844 4845 4846 4847 4848 4849 4850 4851
4852 4853 4854 4855 4856 4857 4858 4859
4860 4861 4862 4863 4864 4865 4866 4867
4868 4869 4870 4871 4872 4873 4874 4875
4876 4877 4878 4879 4880 4881 4882 4883
4884
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ is-
tat partition.img 154
Directory Entry: 154
Not Allocated
File Attributes: File, Archive
Size: 57856
Name: _EPLIC~1.GIF
Directory Entry Times:
Written:  Sun Sep 12 12:44:34 2010
Accessed:  Wed Dec 12 00:00:00 2012
Created:  Sun Sep 12 12:44:34 2010
Sectors:
4772 4773 4774 4775 4776 4777 4778 4779
4780 4781 4782 4783 4784 4785 4786 4787
4788 4789 4790 4791 4792 4793 4794 4795
4796 4797 4798 4799 4800 4801 4802 4803
4804 4805 4806 4807 4808 4809 4810 4811
4812 4813 4814 4815 4816 4817 4818 4819
4820 4821 4822 4823 4824 4825 4826 4827
4828 4829 4830 4831 4832 4833 4834 4835
4836 4837 4838 4839 4840 4841 4842 4843
4844 4845 4846 4847 4848 4849 4850 4851
4852 4853 4854 4855 4856 4857 4858 4859
4860 4861 4862 4863 4864 4865 4866 4867
4868 4869 4870 4871 4872 4873 4874 4875
4876 4877 4878 4879 4880 4881 4882 4883
4884
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Fri 15 Oct 2010 11:13:23 EST
```

D.10 Thumbnail Caches

```
Script started on Fri 15 Oct 2010 09:35:36 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rl disk-part2.img | grep -i thumbs
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fls -
rl disk-part2.img | grep -i thumbs[Kcache
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Fri 15 Oct 2010 09:36:30 EST
```

D.11 Web Browser

```
Script started on Fri 15 Oct 2010 13:45:54 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sudo mount -
o ro,loop disk-part2.img /mnt/
[sudo] password for dleigh:
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cd /[K/mnt/KJ[K[KJohn\ S/h[K
Application Data/ Favorites/        NetHood/          SendTo/
Cookies/          Local Settings/   PrintHood/        Start Menu/
Desktop/          My Documents/     Recent/           Templates/
[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cd /mnt/John\ S/F[KFavorites/
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ ls
[0m[01;32mDesktop.ini[0m
[01;32mhttp--headsteadi.com-wp-content-uploads-2008-04-replica_state_license_plate.gif.url[0m
[01;34mLinks[0m
[01;32mMSN.com.url[0m
[01;32mRadio Station Guide.url[0m
[m]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ file *
Desktop.ini:                                                                    ASCII text, with CRLF line ter-
minators
http--headsteadi.com-wp-content-uploads-2008-04-
replica_state_license_plate.gif.url: ASCII text, with CRLF line terminators
Links:                                                                          directory
MSN.com.url:                                                                    MS Win-
dows 95 Internet shortcut text (URL=< >)
Radio Station Guide.url:                                                        MS Win-
dows 95 Internet shortcut text (URL=< >)
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ cat Desk-
top.ini
[.ShellClassInfo]
IconFile=%SystemRoot%\system32\SHELL32.dll
IconIndex=-173
LocalizedResourceName=@shell32.dll,-12693
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ cat ([K*[KMSN.co
[InternetShortcut]
URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=IStart
Modified=60D3D3690B4DCB0193
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ cat Ra-
dio\ Station\ Guide.url
[InternetShortcut]
URL=http://www.microsoft.com/isapi/redir.dll?prd=windows&sbp=mediaplayer&plcid=&pver=6.1&os=&over=&olcid=&clcid=&ar=Me
Modified=005AD5690B4DCB01BC
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ cat http-
-headsteadi.com-wp-content-uploads-2008-04-replica_state_llicense_plate.gif.url
[DEFAULT]
BASEURL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
[InternetShortcut]
URL=http://headsteadi.com/wp-content/uploads/2008/04/replica_state_license_plate.gif
Modified=B06E4980114DCB0111
IconFile=http://headsteadi.com/favicon.ico
IconIndex=1
]0;dleigh@alphonse: /mnt/John S/Favorites[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites[00m$ cd Links/
]0;dleigh@alphonse: /mnt/John S/Favorites/Links[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites/Links[00m$ ls
[0m[01;32mCustomize Links.url[0m  [01;32mFree Hotmail.url[0m  [01;32mWindows Market-
place.url[0m  [01;32mWindows Media.url[0m  [01;32mWindows.url[0m
[m]0;dleigh@alphonse: /mnt/John S/Favorites/Links[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites/Links[00m$ fi
Customize Links.url:     MS Windows 95 Internet shortcut text (URL=< >)
Free Hotmail.url:        MS Windows 95 Internet shortcut text (URL=< >)
Windows Marketplace.url: MS Windows 95 Internet shortcut text (URL=< >)
Windows Media.url:       MS Windows 95 Internet shortcut text (URL=< >)
Windows.url:             MS Windows 95 Internet shortcut text (URL=< >)
]0;dleigh@alphonse: /mnt/John S/Favorites/Links[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites/Links[00m$ cat
[InternetShortcut]
URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=CLinks
Modified=909BDB690B4DCB0193
[InternetShortcut]
URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail
Modified=3022DD690B4DCB01BC
[InternetShortcut]
URL=http://go.microsoft.com/fwlink/?LinkId=30857&clcid=0x409
IconIndex=107
IconFile=C:\WINDOWS\system32\moricons.dll
Modified=60FF31670B4DCB011B
[InternetShortcut]
```

```
URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windowsmedia
Modified=3022DD690B4DCB01BC
[InternetShortcut]
URL=http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows
Modified=3022DD690B4DCB01BC
]0;dleigh@alphonse: /mnt/John S/Favorites/Links[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Favorites/Links[00m$ exit
exit
Script done on Fri 15 Oct 2010 13:49:32 EST
```

D.11.1 Browser History

```
Script started on Fri 15 Oct 2010 14:08:40 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cd /mnt/John\ S/
]0;dleigh@alphonse: /mnt/John S[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S[00m$ mount | grep mnt
/dev/loop0 on /mnt type vfat (ro)
]0;dleigh@alphonse: /mnt/John S[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S[00m$ cd Lo-
cal\ Settings/History/
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/History[00m$ ll
total 1
-rwxr-xr-x 1 root root 113 2012-12-12 11:12 [0m[01;32mdesktop.ini[0m
drwxr-xr-x 3 root root 512 2012-12-12 11:12 [01;34mHistory.IE5[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History[00m$ cat desktop.ini
[.ShellClassInfo]
UICLSID={7BD29E00-76C1-11CF-9DD0-00A0C9034933}
CLSID={FF393560-C2A7-11CF-BFF4-444553540000}
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/History[00m$ cd His-
tory.IE5/
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ ll
total 65
-rwxr-xr-x 1 root root   113 2012-12-12 11:12 [0m[01;32mdesktop.ini[0m
-rwxr-xr-x 1 root root 65536 2012-12-12 11:12 [01;32mindex.dat[0m
drwxr-xr-x 2 root root   512 2012-12-12 11:12 [01;34mMSHist012010090620100907[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ file *([K
desktop.ini:              ASCII text, with CRLF line terminators
index.dat:                Internet Explorer cache file version Ver 5.2
MSHist012010090620100907: directory
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ cat desktop.ini
[.ShellClassInfo]
UICLSID={7BD29E00-76C1-11CF-9DD0-00A0C9034933}
CLSID={FF393560-C2A7-11CF-BFF4-444553540000}
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco index.dat
History File: index.dat Version: 5.2
TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
URL Visited: John S@http://www.melbourneairport.com.au/To-From-the-Airport.html
09/06/2010 01:28:15 09/06/2010 01:28:15
URL Visited: John S@http://www.bangkokairportonline.com/node/56 09/06/2010 01:31:55
09/06/2010 01:31:55
URL Visited: John S@http://www.humantrafficking.org/updates 09/06/2010 01:37:28
09/06/2010 01:37:28
URL Visited: John S@http://www.bangkokairportonline.com 09/06/2010 01:31:11 09/06/2010 01:31:11

URL Visited: John S@http://www.bangkokairportonline.com/node/51 09/06/2010 01:32:00
09/06/2010 01:32:00
URL Visited: John S@http://www.malaysiaairlines.com/my/en/home.aspx 09/06/2010 01:34:21
09/06/2010 01:34:21
URL Visited: John S@file://10.0.0.2/transfer/Links.txt 09/06/2010 01:43:18 09/06/2010 01:43:18
URL Visited: John S@http://www.qantas.com.au/travel/airlines/home/detect-context
09/06/2010 01:35:09 09/06/2010 01:35:09
URL Visited: John S@javascript:genWIN('http://flight.klia.com.my'); 09/06/2010 01:29:55
09/06/2010 01:29:55
```

URL Visited: John S@http://www.bangkokairportonline.com/node/43 09/06/2010 01:33:47
09/06/2010 01:33:47
URL Visited: John S@http://www.bangkokairportonline.com/node/20 09/06/2010 01:31:38
09/06/2010 01:31:38
URL Visited: John S@http://www.bangkokairportonline.com/node/54 09/06/2010 01:32:11
09/06/2010 01:32:11
URL Visited: John S@http://www.bangkokairportonline.com/taxonomy/term/1 09/06/2010 01:31:36
09/06/2010 01:31:36
URL Visited: John S@http://www.humantrafficking.org/countries/thailand 09/06/2010 01:37:19
09/06/2010 01:37:19
URL Visited: John S@http://www.humantrafficking.org.au 09/06/2010 01:38:53 09/06/2010 01:38:53
URL Visited: John S@http://www.melbourneairport.com.au/Flight-Passenger-Info.html
09/06/2010 01:28:37 09/06/2010 01:28:37
URL Visited: John S@http://www.law.uq.edu.au/human-trafficking-statistics 09/06/2010 01:36:16
09/06/2010 01:36:16
URL Visited: John S@http://internationalaffairs.suite101.com/article.cfm/current
09/06/2010 01:38:50 09/06/2010 01:38:50
URL Visited: John S@http://www.melbourneairport.com.au/Shopping-Eating.html 09/06/2010 01:28:35
09/06/2010 01:28:35
URL Visited: John S@http://www.projectrespect.org.au 09/06/2010 01:38:57 09/06/2010 01:38:57
URL Visited: John S@http://www.klia.com.my/index.php?ch=88&pg=251 09/06/2010 01:33:31
09/06/2010 01:33:31
URL Visited: John S@http://www.bangkokairportonline.com/node/55 09/06/2010 01:31:46
09/06/2010 01:31:46
URL Visited: John S@http://www.bangkokairportonline.com/node/53 09/06/2010 01:31:48
09/06/2010 01:31:48
URL Visited: John S@http://www.suite101.com/internationalaffairs 09/06/2010 01:40:15
09/06/2010 01:40:15
URL Visited: John S@http://www.melbourneairport.com.au/Flight-Passenger-Info/Flight-
Information.html 09/06/2010 01:28:38 09/06/2010 01:28:38

URL Visited: John S@http://www.bangkokairportonline.com/node/23 09/06/2010 01:32:20
09/06/2010 01:32:20
URL Visited: John S@http://www.bigpondsitehelp.com/assist.php?url=www.humantrafficking.org.au
09/06/2010 01:38:58 09/06/2010 01:38:58
URL Visited: John S@http://www.humantrafficking.org/updates/875 09/06/2010 01:37:30
09/06/2010 01:37:30
URL Visited: John S@http://www.pattayadailynews.com/en/2010/02/07/human-trafficking-warrant-
issued-for-arrest-of-woman 09/06/2010 01:44:14 09/06/2010 01:44:14

URL Visited: John S@http://ninemsn.com.au/?ocid=iefvrt&rf=true 09/06/2010 01:15:31
09/06/2010 01:15:31
URL Visited: John S@https://www.google.com/accounts/ServiceLoginAuth 09/06/2010 01:42:56
09/06/2010 01:42:56
URL Visited: John S@http://www.bangkokairportonline.com/node/129 09/06/2010 01:31:31
09/06/2010 01:31:31
URL Visited: John S@http://www.qantas.com.au/travel/airlines/business-solutions/global/en
09/06/2010 01:35:17 09/06/2010 01:35:17
URL Visited: John S@http://www.unicef.org/infobycountry/index.html 09/06/2010 01:39:48
09/06/2010 01:39:48
URL Visited: John S@http://www.google.com.au 09/06/2010 01:47:37 09/06/2010 01:47:37
URL Vis-
ited: John S@http://www.qantas.com.au/info/pms/qantasDomesticInflightEntertainment?int_cam=au:comps:promo:sme-
inflight-advertising:lang:en 09/06/2010 01:35:08 09/06/2010 01:35:08

URL Visited: John S@http://www.humantrafficking.org/countries/australia 09/06/2010 01:37:34
09/06/2010 01:37:34
URL Visited: John S@http://www.melbourneairport.com.au/Flight-Passenger-Info/Flight-
Information/Current-Flights.html 09/06/2010 01:28:48 09/06/2010 01:28:48

URL Visited: John S@http://www.bangkokairportonline.com/node/14 09/06/2010 01:31:41
09/06/2010 01:31:41
URL Visited: John S@http://www.melbourneairport.com.au/To-From-the-Airport/Overview.html
09/06/2010 01:28:16 09/06/2010 01:28:16
URL Visited: John S@http://flight.klia.com.my/fids.aspx 09/06/2010 01:30:45 09/06/2010 01:30:45

URL Visited: John S@http://www.melbourneairport.com.au/Shopping-Eating/Overview.html
09/06/2010 01:28:36 09/06/2010 01:28:36
URL Visited: John S@http://www.antislavery.org.au/resources/legal-resources.html
09/06/2010 01:38:59 09/06/2010 01:38:59
URL
Visited: John S@http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi338.aspx
09/06/2010 01:37:39 09/06/2010 01:37:39

URL Visited: John S@http://www.bangkokairportonline.com/node/141 09/06/2010 01:32:06
09/06/2010 01:32:06
URL Visited: John S@http://www.actnow.com.au/Issues/Human_trafficking.aspx 09/06/2010 01:38:36
09/06/2010 01:38:36
URL Visited: John S@http://www.humantrafficking.org/updates/857 09/06/2010 01:37:02
09/06/2010 01:37:02
URL Visited: John S@http://www.aic.gov.au/documents/7/B/A/{7BA2B075-9282-4331-98A6-
14080E701B2B}tandi338.pdf 09/06/2010 01:38:08 09/06/2010 01:38:08

URL Visited: John S@http://www.bangkokpost.com/advance-search/?papers_sec_id=1
09/06/2010 01:41:14 09/06/2010 01:41:14
URL Vis-
ited: John S@file:///C:/Documents%20and%20Settings/John%20S/Desktop/replica_state_license_plate.gif
09/06/2010 01:47:07 09/06/2010 01:47:07
URL Visited: John S@http://www.unicef.org/protection/index_exploitatio 09/06/2010 01:39:18
09/06/2010 01:39:18
URL Vis-
ited: John S@http://www.malaysiaairlines.com/my/en/home.aspx?selCntry=au&selLocale=en&chkRem=on
09/06/2010 01:34:38 09/06/2010 01:34:38
URL
Visited: John S@http://www.malaysiaairlines.com/au/en/dest/offers/special/special-offers.aspx
09/06/2010 01:34:44 09/06/2010 01:34:44
URL Visited: John S@http://www.klia.com.my/index.php?ch=88 09/06/2010 01:30:53
09/06/2010 01:30:53
URL Visited: John S@http://www.bangkokairportonline.com/node/42 09/06/2010 01:33:20
09/06/2010 01:33:20
URL Visited: John S@http://go.microsoft.com/fwlink/?LinkId=54729&clcid=0x0c09
09/06/2010 01:43:52 09/06/2010 01:43:52
URL Visited: John S@http://www.malaysiaairlines.com/au/en/home.aspx 09/06/2010 01:34:40
09/06/2010 01:34:40
URL Visited: John S@http://www.qantas.com.au/travel/airlines/home/au/en 09/06/2010 01:35:12
09/06/2010 01:35:12
URL Vis-
ited: John S@file:///C:/Documents%20and%20Settings/John%20S/My%20Documents/replica_state_license_plate.gif
09/06/2010 01:45:59 09/06/2010 01:45:59
URL Visited: John S@http://projectrespect.org.au 09/06/2010 01:39:05 09/06/2010 01:39:05
URL Visited: John S@https://login.yahoo.com/config/login_verify2?&.src=ym 09/06/2010 01:47:46
09/06/2010 01:47:46
URL Visited: John S@http://flight.klia.com.my 09/06/2010 01:30:04 09/06/2010 01:30:04
URL Visited: John S@http://headsteadi.com/wp-
content/uploads/2008/04/replica_state_license_plate.gif 09/06/2010 01:46:27 09/06/2010 01:46:27

URL Visited: John S@http://ninemsn.com.au/?ocid=iefvrt 09/06/2010 01:43:52 09/06/2010 01:43:52
URL Visited: John S@http://www.unodc.org/unodc/en/human 09/06/2010 01:39:16 09/06/2010 01:39:16

URL Vis-
ited: John S@https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmai
09/06/2010 01:42:26 09/06/2010 01:42:26
URL Visited: John S@http://www.melbourneairport.com.au/Flight-Passenger-Info/Overview.html
09/06/2010 01:28:37 09/06/2010 01:28:37
URL Visited: John S@http://www.bangkokairportonline.com/node/15 09/06/2010 01:31:29
09/06/2010 01:31:29
URL Visited: John S@http://www.mizzima.com/news/regional/1936-two-human-traffickers-arrested-
in-thailand.html 09/06/2010 01:41:27 09/06/2010 01:41:27

URL Visited: John S@http://www.aic.gov.au/en/publications/current%20series/tandi/321-
340/tandi338/view%20paper.aspx 09/06/2010 01:38:24 09/06/2010 01:38:24

URL Visited: John S@javascript: submitctyform() 09/06/2010 01:34:38 09/06/2010 01:34:38
URL Visited: John S@http://www.dfat.gov.au/dept/annual_reports/04_05 09/06/2010 01:38:56
09/06/2010 01:38:56
URL Visited: John S@http://www.bangkokairportonline.com/node/52 09/06/2010 01:32:04
09/06/2010 01:32:04
URL
Visited: John S@http://www.malaysiaairlines.com/my/en/dest/offers/special/special-offers.aspx
09/06/2010 01:34:08 09/06/2010 01:34:08
URL Visited: John S@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
09/06/2010 01:43:53 09/06/2010 01:43:53
URL Visited: John S@http://www.antislavery.org.au/solutions/policy.html 09/06/2010 01:38:47
09/06/2010 01:38:47
URL Visited: John S@http://www.humantrafficking.org/updates/10 09/06/2010 01:37:04
09/06/2010 01:37:04
URL Visited: John S@http://www.bangkokairportonline.com/node/50 09/06/2010 01:32:03

```
09/06/2010 01:32:03
URL Visited: John S@http://www.melbourneairport.com.au 09/06/2010 01:33:20 09/06/2010 01:33:20
URL Visited: John S@about:Home 09/06/2010 01:02:46 09/06/2010 01:02:46
URL Visited: John S@http://www.bangkokairportonline.com/node/13 09/06/2010 01:31:26
09/06/2010 01:31:26
URL Visited: John S@http://www.bangkokairportonline.com/node/41 09/06/2010 01:32:32
09/06/2010 01:32:32
URL Visited: John S@http://www.bangkokpost.com/news/local/193458/spanish-sex-ring-exposed
09/06/2010 01:40:46 09/06/2010 01:40:46
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ cd MSHist012010090620100907/
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[00m$ pasco index.dat  [A
History File: index.dat Version: 5.2
TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
URL
:2010090620100907: John S@http://www.malaysiaairlines.com/au/en/dest/offers/special/special-
offers.aspx 09/06/2010 11:34:44
09/06/2010 01:34:44
URL :2010090620100907: John S@http://flight.klia.com.my 09/06/2010 11:30:04 09/06/2010 01:30:04
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/13 09/06/2010 11:31:26
09/06/2010 01:31:26
URL :2010090620100907: John S@http://www.humantrafficking.org/countries/thailand
09/06/2010 11:37:19 09/06/2010 01:37:19
URL
:2010090620100907: John S@file:///C:/Documents%20and%20Settings/John%20S/My%20Documents/replica_state_license_plate.gi
09/06/2010 11:45:59 09/06/2010 01:45:59
URL :2010090620100907: John S@http://internationalaffairs.suite101.com/article.cfm/current
09/06/2010 11:38:50 09/06/2010 01:38:50
URL :2010090620100907: John S@http://www.dfat.gov.au/dept/annual_reports/04_05
09/06/2010 11:38:56 09/06/2010 01:38:56
URL :2010090620100907: John S@http://www.pattayadailynews.com/en/2010/02/07/human-trafficking-
warrant-issued-for-arrest-of-woman 09/06/2010 11:44:14
09/06/2010 01:44:14
URL :2010090620100907: John S@http://www.melbourneairport.com.au/Flight-Passenger-
Info/Overview.html 09/06/2010 11:28:37
09/06/2010 01:28:37
URL :2010090620100907: John S@:Host: www.law.uq.edu.au 09/06/2010 11:36:16 09/06/2010 01:36:16
URL :2010090620100907: John S@http://www.mizzima.com/news/regional/1936-two-human-traffickers-
arrested-in-thailand.html 09/06/2010 11:41:27
09/06/2010 01:41:27
URL :2010090620100907: John S@http://www.aic.gov.au/en/publications/current%20series/tandi/321-
340/tandi338/view%20paper.aspx 09/06/2010 11:38:24
09/06/2010 01:38:24
URL :2010090620100907: John S@:Host: headsteadi.com 09/06/2010 11:45:37 09/06/2010 01:45:37
URL :2010090620100907: John S@http://www.aic.gov.au/publications/current%20series/tandi/321-
340/tandi338.aspx 09/06/2010 11:37:39
09/06/2010 01:37:39
URL :2010090620100907: John S@:Host: www.antislavery.org.au 09/06/2010 11:38:47
09/06/2010 01:38:47
URL :2010090620100907: John S@http://projectrespect.org.au 09/06/2010 11:39:05
09/06/2010 01:39:05
URL :2010090620100907: John S@:Host: www.projectrespect.org.au 09/06/2010 11:38:57
09/06/2010 01:38:57
URL :2010090620100907: John S@http://headsteadi.com/wp-
content/uploads/2008/04/replica_state_license_plate.gif 09/06/2010 11:45:37
09/06/2010 01:45:37
URL
:2010090620100907: John S@http://www.melbourneairport.com.au/To-From-the-Airport/Overview.html
09/06/2010 11:28:16 09/06/2010 01:28:16
URL :2010090620100907: John S@http://www.humantrafficking.org/updates/10 09/06/2010 11:37:04
09/06/2010 01:37:04
URL :2010090620100907: John S@https://www.google.com/accounts/ServiceLoginAuth
09/06/2010 11:42:56 09/06/2010 01:42:56
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/56 09/06/2010 11:31:55
09/06/2010 01:31:55
URL :2010090620100907: John S@:Host: www.humantrafficking.org 09/06/2010 11:36:43
09/06/2010 01:36:43
URL :2010090620100907: John S@:Host: www.unicef.org 09/06/2010 11:39:18 09/06/2010 01:39:18
URL :2010090620100907: John S@:Host: www.actnow.com.au 09/06/2010 11:38:36 09/06/2010 01:38:36
URL :2010090620100907: John S@:Host: www.bangkokairportonline.com 09/06/2010 11:31:11
```

```
09/06/2010 01:31:11
URL
:2010090620100907: John S@http://www.qantas.com.au/travel/airlines/business-solutions/global/en
09/06/2010 11:35:17 09/06/2010 01:35:17
URL :2010090620100907: John S@http://www.projectrespect.org.au 09/06/2010 11:38:57
09/06/2010 01:38:57
URL :2010090620100907: John S@:Host: www.bangkokpost.com 09/06/2010 11:40:46
09/06/2010 01:40:46
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/50 09/06/2010 11:32:03
09/06/2010 01:32:03
URL :2010090620100907: John S@http://www.humantrafficking.org/updates 09/06/2010 11:37:28
09/06/2010 01:37:28
URL :2010090620100907: John S@:Host: www.unodc.org 09/06/2010 11:39:16 09/06/2010 01:39:16
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/53 09/06/2010 11:31:48
09/06/2010 01:31:48
URL :2010090620100907: John S@:Host: www.pattayadailynews.com 09/06/2010 11:44:14
09/06/2010 01:44:14
URL :2010090620100907: John S@:Host: www.aic.gov.au 09/06/2010 11:37:39 09/06/2010 01:37:39
URL :2010090620100907: John S@:Host: www.google.com.au 09/06/2010 11:47:37 09/06/2010 01:47:37
URL :2010090620100907: John S@http://ninemsn.com.au/?ocid=iefvrt 09/06/2010 11:26:45
09/06/2010 01:26:45
URL
:2010090620100907: John S@http://www.bigpondsitehelp.com/assist.php?url=www.humantrafficking.org.au
09/06/2010 11:38:58 09/06/2010 01:38:58
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/42 09/06/2010 11:33:20
09/06/2010 01:33:20
URL :2010090620100907: John S@http://www.humantrafficking.org.au 09/06/2010 11:38:53
09/06/2010 01:38:53
URL :2010090620100907: John S@:Host: www.malaysiaairlines.com 09/06/2010 11:34:14
09/06/2010 01:34:14
URL :2010090620100907: John S@:Host: www.google.com 09/06/2010 11:42:26 09/06/2010 01:42:26
URL :2010090620100907: John S@:Host: My Computer 09/06/2010 11:45:59 09/06/2010 01:45:59
URL :2010090620100907: John S@:Host: www.humantrafficking.org.au 09/06/2010 11:38:53
09/06/2010 01:38:53
URL :2010090620100907: John S@http://www.malaysiaairlines.com/au/en/home.aspx
09/06/2010 11:34:40 09/06/2010 01:34:40
URL :2010090620100907: John S@http://www.humantrafficking.org/updates/875 09/06/2010 11:37:30
09/06/2010 01:37:30
URL :2010090620100907: John S@http://www.unicef.org/infobycountry/index.html
09/06/2010 11:39:48 09/06/2010 01:39:48
URL
:2010090620100907: John S@http://www.bangkokpost.com/news/local/193458/spanish-sex-ring-exposed
09/06/2010 11:40:46 09/06/2010 01:40:46
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/51 09/06/2010 11:32:00
09/06/2010 01:32:00
URL :2010090620100907: John S@http://www.antislavery.org.au/resources/legal-resources.html
09/06/2010 11:38:59 09/06/2010 01:38:59
URL :2010090620100907: John S@http://www.humantrafficking.org/countries/australia
09/06/2010 11:37:34 09/06/2010 01:37:34
URL :2010090620100907: John S@http://www.humantrafficking.org/updates/857 09/06/2010 11:37:02
09/06/2010 01:37:02
URL
:2010090620100907: John S@file:///C:/Documents%20and%20Settings/John%20S/Desktop/replica_state_license_plate.gif
09/06/2010 11:47:07 09/06/2010 01:47:07
URL :2010090620100907: John S@http://www.klia.com.my/index.php?ch=88&pg=251 09/06/2010 11:33:31
09/06/2010 01:33:31
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/23 09/06/2010 11:32:20
09/06/2010 01:32:20
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/43 09/06/2010 11:33:47
09/06/2010 01:33:47
URL :2010090620100907: John S@http://www.law.uq.edu.au/human-trafficking-statistics
09/06/2010 11:36:16 09/06/2010 01:36:16
URL :2010090620100907: John S@http://www.aic.gov.au/documents/7/B/A/{7BA2B075-9282-4331-98A6-
14080E701B2B}tandi338.pdf 09/06/2010 11:38:08
09/06/2010 01:38:08
URL :2010090620100907: John S@http://flight.klia.com.my/fids.aspx 09/06/2010 11:30:31
09/06/2010 01:30:31
URL :2010090620100907: John S@:Host: www.klia.com.my 09/06/2010 11:31:12 09/06/2010 01:31:12
URL :2010090620100907: John S@:Host: flight.klia.com.my 09/06/2010 11:30:04 09/06/2010 01:30:04
URL :2010090620100907: John S@http://www.melbourneairport.com.au/Flight-Passenger-Info/Flight-
Information/Current-Flights.html 09/06/2010 11:28:48
09/06/2010 01:28:48
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/20 09/06/2010 11:31:38
```

```
09/06/2010 01:31:38
URL :2010090620100907: John S@http://www.unicef.org/protection/index_exploitatio
09/06/2010 11:39:18 09/06/2010 01:39:18
URL :2010090620100907: John S@http://ninemsn.com.au/?ocid=iefvrt&rf=true 09/06/2010 11:15:31
09/06/2010 01:15:31
URL :2010090620100907: John S@http://www.malaysiaairlines.com/my/en/home.aspx
09/06/2010 11:34:21 09/06/2010 01:34:21
URL
:2010090620100907: John S@http://www.qantas.com.au/info/pms/qantasDomesticInflightEntertainment?int_cam=au:comps:promo
inflight-advertising:lang:en 09/06/2010 11:35:08
09/06/2010 01:35:08
URL :2010090620100907: John S@http://www.bangkokairportonline.com 09/06/2010 11:31:11
09/06/2010 01:31:11
URL :2010090620100907: John S@http://www.bangkokairportonline.com/taxonomy/term/1
09/06/2010 11:31:36 09/06/2010 01:31:36
URL :2010090620100907: John S@file://10.0.0.2/transfer/Links.txt 09/06/2010 11:43:18
09/06/2010 01:43:18
URL :2010090620100907: John S@http://www.google.com.au 09/06/2010 11:47:37 09/06/2010 01:47:37
URL :2010090620100907: John S@http://www.antislavery.org.au/solutions/policy.html
09/06/2010 11:38:47 09/06/2010 01:38:47
URL :2010090620100907: John S@http://www.qantas.com.au/travel/airlines/home/au/en
09/06/2010 11:35:12 09/06/2010 01:35:12
URL :2010090620100907: John S@:Host: www.bigpondsitehelp.com 09/06/2010 11:38:58
09/06/2010 01:38:58
URL :2010090620100907: John S@http://www.melbourneairport.com.au 09/06/2010 11:33:20
09/06/2010 01:33:20
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/141 09/06/2010 11:32:06
09/06/2010 01:32:06
URL :2010090620100907: John S@http://www.bangkokpost.com/advance-search/?papers_sec_id=1
09/06/2010 11:41:14 09/06/2010 01:41:14
URL
:2010090620100907: John S@https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=htt
09/06/2010 11:42:26 09/06/2010 01:42:26
URL :2010090620100907: John S@http://www.actnow.com.au/Issues/Human_trafficking.aspx
09/06/2010 11:38:36 09/06/2010 01:38:36
URL :2010090620100907: John S@:Host: www.suite101.com 09/06/2010 11:39:05 09/06/2010 01:39:05
URL :2010090620100907: John S@:Host: www.qantas.com.au 09/06/2010 11:34:57 09/06/2010 01:34:57
URL :2010090620100907: John S@:Host: www.dfat.gov.au 09/06/2010 11:38:55 09/06/2010 01:38:55
URL :2010090620100907: John S@http://www.suite101.com/internationalaffairs 09/06/2010 11:40:15
09/06/2010 01:40:15
URL :2010090620100907: John S@:Host: projectrespect.org.au 09/06/2010 11:39:05
09/06/2010 01:39:05
URL :2010090620100907: John S@:Host: ninemsn.com.au 09/06/2010 11:03:29 09/06/2010 01:03:29
URL :2010090620100907: John S@:Host: www.melbourneairport.com.au 09/06/2010 11:28:09
09/06/2010 01:28:09
URL :2010090620100907: John S@:Host: internationalaffairs.suite101.com 09/06/2010 11:38:50
09/06/2010 01:38:50
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/55 09/06/2010 11:31:46
09/06/2010 01:31:46
URL :2010090620100907: John S@:Host: 10.0.0.2 09/06/2010 11:27:43 09/06/2010 01:27:43
URL :2010090620100907: John S@http://www.melbourneairport.com.au/Shopping-Eating/Overview.html
09/06/2010 11:28:36 09/06/2010 01:28:36
URL :2010090620100907: John S@http://www.unodc.org/unodc/en/human 09/06/2010 11:39:16
09/06/2010 01:39:16
URL :2010090620100907: John S@:Host: www.mizzima.com 09/06/2010 11:41:27 09/06/2010 01:41:27
URL :2010090620100907: John S@http://www.bangkokairportonline.com/node/41 09/06/2010 11:32:32
09/06/2010 01:32:32
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[00m$ ll
total 48
-rwxr-xr-x 1 root root 49152 2012-12-12 11:12 [0m[01;32mindex.dat[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5/MSHist012010090620100907[00m$ cd ..
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ ll
total 65
-rwxr-xr-x 1 root root   113 2012-12-12 11:12 [0m[01;32mdesktop.ini[0m
-rwxr-xr-x 1 root root 65536 2012-12-12 11:12 [01;32mindex.dat[0m
drwxr-xr-x 2 root root   512 2012-12-12 11:12 [01;34mMSHist012010090620100907[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
```

```
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ cd ..
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/History[00m$ ll
total 1
-rwxr-xr-x 1 root root 113 2012-12-12 11:12 [0m[01;32mdesktop.ini[0m
drwxr-xr-x 3 root root 512 2012-12-12 11:12 [01;34mHistory.IE5[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/History[00m$ find .
.
./History.IE5
./History.IE5/MSHist012010090620100907
./History.IE5/MSHist012010090620100907/index.dat
./History.IE5/desktop.ini
./History.IE5/index.dat
./desktop.ini
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/History[00m$ exit
exit
Script done on Fri 15 Oct 2010 14:20:05 EST
Script started on Fri 15 Oct 2010 14:21:51 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cd /mnt/John\ S/LK[Kocal\ Set-
tings/History/History.IE5/
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ ll
total 65
-rwxr-xr-x 1 root root   113 2012-12-12 11:12 [0m[01;32mdesktop.ini[0m
-rwxr-xr-x 1 root root 65536 2012-12-12 11:12 [01;32mindex.dat[0m
drwxr-xr-x 2 root root   512 2012-12-12 11:12 [01;34mMSHist012010090620100907[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco io[Kndex.dat > /var/evidence/urls.1[K[K1
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco MSHist012010090620100907/index.dat  > /var/evidence/urls1 [K[K2
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ exit
exit
Script done on Fri 15 Oct 2010 14:22:41 EST
```

D.11.2 Browser Cache

```
Script started on Sun 17 Oct 2010 15:52:17 EST
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | head
History File: index.dat Version: 5.2
TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
URL http://ninemsn.com.au/share/com/js/tab.js 06/07/2007 14:17:32 09/06/2010 01:43:53 tab[2].js
SP6FOLM3 HTTP/1.1 200 OK  Content-Length: 13643  Content-Type: application/x-javascript
URL http://ninemsn.com.au/img/video/layout/bottom_cnr_right.gif 08/05/2009 14:19:44
09/06/2010 01:26:44 bottom_cnr_right[1].gif K56JOP2V HTTP/1.1 200 OK  Content-
Length: 111  Content-Type: image/gif  ETag: "f679e0f58315ca1:0"  server-
name: web9msn20  P3P: CP="BUS CUR CONi FIN IVDi ONL OUR PHY SAMo"  X-Powered-By: ASP.NET  X-UA-
Compatible: IE=EmulateIE7    ~U:john s
URL
http://data.ninemsn.com.au/NHProfile/GetNHProfile.aspx?ngcResFcn=NHProfile_JSONResult_06f46e1206d930f7c2eced9823971edb
09/06/2010 01:26:42 GetNHProfile[1].htm K56JOP2V
HTTP/1.1 200 OK  Content-Length: 179  Content-Type: text/html
URL http://www.melbourneairport.com.au/images/generic/mainLogo.jpg 06/19/2009 15:18:35
09/06/2010 01:33:18 mainLogo[1].jpg SP6FOLM3 HTTP/1.1 200 OK  Content-Length: 6268  Content-
Type: image/jpeg  ETag: "47a939659df0c91:1351e"  X-Powered-By: ASP.NET    ~U:john s
URL http://flight.klia.com.my/fids.aspx1f8a74ad 09/06/2010 01:30:27 fids[1].htm I9EFGXI7
HTTP/1.1 200 OK  X-Powered-By: ASP.NET  X-AspNet-Version: 2.0.50727  Content-
Type: text/html; charset=utf-8  Content-Length: 466796    ~U:john s
URL http://www.bangkokairportonline.com/themes/sands_css/bg/header-blue.png 05/26/2006 00:41:26
09/06/2010 01:33:45 header-blue[1].png K56JOP2V
HTTP/1.1 200 OK  ETag: "f7f844a-a9-4475c216"  Content-Length: 169  Keep-
Alive: timeout=1, max=9996  Content-Type: image/png    ~U:john s
URL http://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-
6916631509554610&format=160x600_as&output=html&h=600&w=160&lmt=1283700690&channel=7827273770&ad_type=text_image&alt_co
```

```
6650868-
3&u_tz=600&u_his=4&u_java=1&u_h=778&u_w=1440&u_ah=748&u_aw=1440&u_cd=32&u_nplug=0&u_nmime=0&biw=1419&bih=609&eid=44901
09/06/2010 01:31:31 CAUN45U3.htm G92JOPQV
HTTP/1.1 200 OK  Content-Length: 13983  Content-Type: text/html
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | wc
   1710   36505  528444
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | cut -f 4 | head -5
History File: index.dat Version: 5.2
ACCESS TIME
09/06/2010 01:43:53
09/06/2010 01:26:44
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | cut -f 4 | sort -n | uniq | head -5
ACCESS TIME
History File: index.dat Version: 5.2
09/06/2010 01:03:25
09/06/2010 01:03:26
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | cut -f 4 | sort -n | uniq | tail -5
09/06/2010 01:47:36
09/06/2010 01:47:37
09/06/2010 01:47:44
09/06/2010 01:47:45
09/06/2010 01:47:46
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ exit
exit
Script done on Sun 17 Oct 2010 15:54:27 EST
Script started on Sun 17 Oct 2010 15:55:41 EST
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | cut -d / -f3 | head
History File: index.dat Version: 5.2
TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
ninemsn.com.au
ninemsn.com.au
data.ninemsn.com.au
www.melbourneairport.com.au
flight.klia.com.my
www.bangkokairportonline.com
googleads.g.doubleclick.net
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | cut -d / -f3 | sort | uniq -c | sort -n
      1
      1 2010 01:41:00 09
      1 ad.doubleclick.net
      1 ads1.msads.net
      1 ads1.msn.com
      1 ads2.msads.net
      1 adsfac.net
      1 a.tribalfusion.com
      1 banner.synergy-e.com
      1 b.rad.msn.com
      1 b.static.ak.fbcdn.net
      1 buttons.googlesyndication.com
      1 cdn.netvibes.com
      1 connect.facebook.net
      1 download.macromedia.com
      1 ec.atdmt.com
      1 edge.quantserve.com
      1 fpdownload2.macromedia.com
      1 graphics.suite101.com.s3.amazonaws.com
      1 History File: index.dat Version: 5.2
      1 map.media6degrees.com
      1 myfeeds.aolcdn.com
```

```
 1 rmd.atdmt.com
 1 sc.msn.com
 1 spe.atdmt.com
 1 ssl.google-analytics.com
 1 static.addtoany.com
 1 static.fbshare.me
 1 static.technorati.com
 1 tags.expo9.exponential.com
 1 tweetmeme.com
 1 TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
 1 us.i1.yimg.com
 1 webrank.truehits.net
 1 www.bing.com
 1 www.bloglines.com
 1 www.flightstats.com
 1 www.googleadservices.com
 1 www.gstatic.com
 1 www.humantrafficking.org.au
 1 www.microsoft.com
 1 www.netvibes.com
 1 www.newsgator.com
 1 www.statcounter.com
 1 www.suite101.com
 1 yahoomail.com
 2 a.ads2.msads.net
 2 addoer.com
 2 ads.ninemsn.com.au
 2 api.tweetmeme.com
 2 a.rad.msn.com
 2 b.scorecardresearch.com
 2 hits.truehits.in.th
 2 login.yahoo.com
 2 media1.bangkokpost.com
 2 partner.googleadservices.com
 2 pubads.g.doubleclick.net
 2 rad.msn.com
 2 secure-au.imrworldwide.com
 2 video.ninemsn.com.au
 2 www.google-analytics.com
 2 zulu.tweetmeme.com
 3 bs.serving-sys.com
 3 www.clocklink.com
 4 ad.au.doubleclick.net
 4 headsteadi.com
 4 s0.2mdn.net
 4 tap-cdn.rubiconproject.com
 4 www.ag.gov.au
 4 www.google.com.au
 5 static2.suite101.com
 5 static.ak.fbcdn.net
 5 widgets.fbshare.me
 6 mail.google.com
 6 www.uq.edu.au
 7 ads.bangkokpost.co.th
 7 ajaxsearch.partners.agoda.com
 7 lvs.truehits.in.th
 7 s7.addthis.com
 7 www.dfat.gov.au
 7 www.unodc.org
 8 ds.serving-sys.com
 8 shared.9msn.com.au
 9 data.ninemsn.com.au
 9 s.yimg.com
 9 www.google.com
11 images.ninemsn.com.au
11 pagead2.googlesyndication.com
11 www.bigpondsitehelp.com
14 graphics.suite101.com
15 www.neoskosmos.com
17 images.suite101.com
22 www.law.uq.edu.au
23 www.humantrafficking.org
24 www.aic.gov.au
```

```
     25 c.statcounter.com
     25 projectrespect.org.au
     37 www.antislavery.org.au
     41 www.mizzima.com
     47 9msn.com.au
     54 www.klia.com.my
     63 www.pattayadailynews.com
     64 www.actnow.com.au
     68 www.bangkokpost.com
     74 googleads.g.doubleclick.net
     75 flight.klia.com.my
     83 www.bangkokairportonline.com
     99 www.melbourneairport.com.au
    105 www.qantas.com.au
    112 www.unicef.org
    143 ninemsn.com.au
    227 www.malaysiaairlines.com
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ exit
exit
Script done on Sun 17 Oct 2010 15:56:56 EST
Script started on Sun 17 Oct 2010 16:03:09 EST
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ pasco index.dat | grep - i pdf
URL http://www.aic.gov.au/images/template/icon_pdf.png 02/18/2009 11:18:17 09/06/2010 01:38:24
icon_pdf[1].png G92J0PQV HTTP/1.1 200 OK  Content-Type: image/png  ETag: "d43d0655e91c91:0"  X-
Powered-By: ASP.NET  Content-Length: 591    ~U:john s
URL http://www.mizzima.com/templates/ja_vauxite/images/pdf_button.png 06/06/2009 22:04:16
09/06/2010 01:41:24 pdf_button[1].png SP6FOLM3
HTTP/1.1 200 OK  ETag: "1b1ceaa-1e9-46baccedd5000"  Content-Length: 489  Keep-
Alive: timeout=15, max=92  Content-Type: image/png    ~U:john s
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files/Content.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary In-
ternet Files/Content.IE5[00m$ cd ..
]0;dleigh@alphonse: /mnt/John S/Local Settings/Temporary Inter-
net Files[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings/Temporary Inter-
net Files[00m$ cd ..
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Settings[00m$ cd ..
]0;dleigh@alphonse: /mnt/John S[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S[00m$ cd Hi[K[KLocal\ Set-
tings/History/History.IE5/
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ ls
[0m[01;32mdesktop.ini[0m  [01;32mindex.dat[0m  [01;34mMSHist012010090620100907[0m
[m]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco index.dat | grep -i pdf
URL Visited: John S@http://www.aic.gov.au/documents/7/B/A/{7BA2B075-9282-4331-98A6-
14080E701B2B}tandi338.pdf 09/06/2010 01:38:08 09/06/2010 01:38:08

]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco
desktop.ini               index.dat                 MSHist012010090620100907/
[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ pasco MSHist012010090620100907/index.dat  | grep -i pdf
URL :2010090620100907: John S@http://www.aic.gov.au/documents/7/B/A/{7BA2B075-9282-4331-98A6-
14080E701B2B}tandi338.pdf 09/06/2010 11:38:08
09/06/2010 01:38:08
]0;dleigh@alphonse: /mnt/John S/Local Set-
tings/History/History.IE5[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Local Set-
tings/History/History.IE5[00m$ exit
exit
Script done on Sun 17 Oct 2010 16:04:14 EST
```

D.11.3 Cookies

```
Script started on Sun 17 Oct 2010 16:48:40 EST
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ ls -
1  | wc
```

```
     58     115    1595
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ pasco in-
dex.dat | wc
     60     528    6197
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ pasco in-
dex.dat
History File: index.dat Version: 5.2
TYPE URL MODIFIED TIME ACCESS TIME FILENAME DIRECTORY HTTP HEADERS
URL Cookie:john s@tap.rubiconproject.com/ 09/06/2010 01:40:18 09/06/2010 01:40:18
john s@tap.rubiconproject[2].txt
URL Cookie:john s@statcounter.com/ 09/06/2010 01:33:46 09/06/2010 01:33:46
john s@statcounter[1].txt
URL Cookie:john s@www.pattayadailynews.com/ 09/06/2010 01:44:22 09/06/2010 01:44:22
john s@www.pattayadailynews[2].txt
URL Cookie:john s@www.melbourneairport.com.au/ 09/06/2010 01:28:05 09/06/2010 01:28:05
john s@www.melbourneairport.com[1].txt
URL Cookie:john s@scorecardresearch.com/ 09/06/2010 01:40:15 09/06/2010 01:40:15
john s@scorecardresearch[1].txt
URL Cookie:john s@tribalfusion.com/ 09/06/2010 01:40:14 09/06/2010 01:40:14
john s@tribalfusion[1].txt
URL Cookie:john s@lvs.truehits.in.th/ 09/06/2010 01:40:38 09/06/2010 01:44:13
john s@lvs.truehits.in[2].txt
URL Cookie:john s@telstra.com/ 09/06/2010 01:38:58 09/06/2010 01:38:58 john s@telstra[1].txt
URL Cookie:john s@qantas.com.au/ 09/06/2010 01:34:57 09/06/2010 01:34:57
john s@qantas.com[1].txt
URL Cookie:john s@unodc.org/ 09/06/2010 01:39:20 09/06/2010 01:39:20 john s@unodc[2].txt
URL Cookie:john s@melbourneairport.com.au/ 09/06/2010 01:33:18 09/06/2010 01:33:18
john s@melbourneairport.com[1].txt
URL Cookie:john s@www.bigpondsitehelp.com/ 09/06/2010 01:38:54 09/06/2010 01:38:54
john s@www.bigpondsitehelp[1].txt
URL Cookie:john s@overture.com/ 09/06/2010 01:26:43 09/06/2010 01:26:43 john s@overture[2].txt
URL Cookie:john s@www.malaysiaairlines.com/ 09/06/2010 01:34:38 09/06/2010 01:34:38
john s@www.malaysiaairlines[2].txt
URL Cookie:john s@www.law.uq.edu.au/ 09/06/2010 01:36:14 09/06/2010 01:36:14
john s@www.law.uq.edu[1].txt
URL Cookie:john s@pattayadailynews.com/ 09/06/2010 01:45:37 09/06/2010 01:45:37
john s@pattayadailynews[1].txt
URL Cookie:john s@google.com.au/ 09/06/2010 01:47:36 09/06/2010 01:47:36
john s@google.com[1].txt
URL Cookie:john s@doubleclick.net/ 09/06/2010 01:15:30 09/06/2010 01:44:11
john s@doubleclick[1].txt
URL Cookie:john s@www.antislavery.org.au/ 09/06/2010 01:38:49 09/06/2010 01:38:49
john s@www.antislavery.org[1].txt
URL Cookie:john s@bangkokpost.com/ 09/06/2010 01:41:21 09/06/2010 01:41:21
john s@bangkokpost[1].txt
URL Cookie:john s@suite101.com/ 09/06/2010 01:40:13 09/06/2010 01:40:13 john s@suite101[1].txt
URL Cookie:john s@rad.msn.com/ 09/06/2010 01:03:25 09/06/2010 01:43:54 john s@rad.msn[2].txt
URL Cookie:john s@www.uq.edu.au/ 09/06/2010 01:36:15 09/06/2010 01:36:15
john s@www.uq.edu[2].txt
URL Cookie:john s@www.bangkokpost.com/ 09/06/2010 01:40:35 09/06/2010 01:40:35
john s@www.bangkokpost[1].txt
URL Cookie:john s@imrworldwide.com/cgi-bin 09/06/2010 01:03:27 09/06/2010 01:26:44
john s@cgi-bin[2].txt
URL Cookie:john s@www.suite101.com/ 09/06/2010 01:38:51 09/06/2010 01:38:51
john s@www.suite101[2].txt
URL Cookie:john s@antislavery.org.au/ 09/06/2010 01:38:54 09/06/2010 01:38:54
john s@antislavery.org[2].txt
URL Cookie:john s@yahoo.com/ 09/06/2010 01:47:41 09/06/2010 01:47:41 john s@yahoo[1].txt
URL Cookie:john s@bigpondsitehelp.com/ 09/06/2010 01:38:58 09/06/2010 01:38:58
john s@bigpondsitehelp[2].txt
URL Cookie:john s@ninemsn.com.au/ 09/06/2010 01:43:54 09/06/2010 01:43:54
john s@ninemsn.com[1].txt
URL Cookie:john s@www.bangkokairportonline.com/ 09/06/2010 01:31:07 09/06/2010 01:31:07
john s@www.bangkokairportonline[1].txt
URL Cookie:john s@projectrespect.org.au/ 09/06/2010 01:39:01 09/06/2010 01:39:01
john s@projectrespect.org[1].txt
URL Cookie:john s@unicef.org/ 09/06/2010 01:39:47 09/06/2010 01:39:47 john s@unicef[1].txt
URL Cookie:john s@serving-sys.com/ 09/06/2010 01:41:08 09/06/2010 01:41:08
john s@serving-sys[2].txt
URL Cookie:john s@addthis.com/ 09/06/2010 01:35:09 09/06/2010 01:35:09 john s@addthis[2].txt
URL Cookie:john s@internationalaffairs.suite101.com/ 09/06/2010 01:38:50 09/06/2010 01:38:50
john s@internationalaffairs.suite101[2].txt
URL Cookie:john s@google.com/ 09/06/2010 01:47:36 09/06/2010 01:47:36 john s@google[2].txt
```

```
URL Cookie:john s@bangkokairportonline.com/ 09/06/2010 01:33:46 09/06/2010 01:33:46
john s@bangkokairportonline[1].txt
URL Cookie:john s@atdmt.com/ 09/06/2010 01:03:28 09/06/2010 01:26:44 john s@atdmt[1].txt
URL Cookie:john s@google.com/mail/help/ 09/06/2010 01:42:56 09/06/2010 01:47:36
john s@help[2].txt
URL Cookie:john s@humantrafficking.org/ 09/06/2010 01:37:34 09/06/2010 01:37:34
john s@humantrafficking[1].txt
URL Cookie:john s@www.mizzima.com/ 09/06/2010 01:41:21 09/06/2010 01:41:21
john s@www.mizzima[1].txt
URL Cookie:john s@mizzima.com/ 09/06/2010 01:41:25 09/06/2010 01:41:25 john s@mizzima[2].txt
URL Cookie:john s@www.aic.gov.au/ 09/06/2010 01:38:23 09/06/2010 01:38:23
john s@www.aic.gov[2].txt
URL Cookie:john s@aic.gov.au/ 09/06/2010 01:38:24 09/06/2010 01:38:24 john s@aic.gov[2].txt
URL Cookie:john s@unitus.synergy-e.com/ 09/06/2010 01:41:13 09/06/2010 01:41:13
john s@unitus.synergy-e[2].txt
URL Cookie:john s@malaysiaairlines.112.2o7.net/ 09/06/2010 01:34:04 09/06/2010 01:34:04
john s@malaysiaairlines.112.2o7[1].txt
URL Cookie:john s@msnportal.112.2o7.net/ 09/06/2010 01:03:28 09/06/2010 01:26:44
john s@msnportal.112.2o7[1].txt
URL Cookie:john s@adsfac.net/ 09/06/2010 01:03:29 09/06/2010 01:03:29 john s@adsfac[2].txt
URL Cookie:john s@www.qantas.com.au/ 09/06/2010 01:35:10 09/06/2010 01:35:10
john s@www.qantas.com[1].txt
URL Cookie:john s@google.com/accounts/ 09/06/2010 01:42:56 09/06/2010 01:47:36
john s@accounts[1].txt
URL Cookie:john s@c.ninemsn.com.au/ 09/06/2010 01:03:29 09/06/2010 01:26:44
john s@c.ninemsn.com[1].txt
URL Cookie:john s@quantserve.com/ 09/06/2010 01:38:55 09/06/2010 01:38:55
john s@quantserve[1].txt
URL Cookie:john s@rubiconproject.com/ 09/06/2010 01:40:18 09/06/2010 01:40:18
john s@rubiconproject[2].txt
URL Cookie:john s@neoskosmos.com/ 09/06/2010 01:39:57 09/06/2010 01:39:57
john s@neoskosmos[1].txt
URL Cookie:john s@actnow.com.au/ 09/06/2010 01:38:35 09/06/2010 01:38:35
john s@actnow.com[1].txt
URL Cookie:john s@bs.serving-sys.com/ 09/06/2010 01:41:08 09/06/2010 01:41:08
john s@bs.serving-sys[2].txt
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ pasco in-
dex.dat | cut -f4 | sort -n | head -5
ACCESS TIME
History File: index.dat Version: 5.2
09/06/2010 01:03:29
09/06/2010 01:26:43
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$  pasco in-
dex.dat | cut -f4 | sort -n | tail -5
09/06/2010 01:47:36
09/06/2010 01:47:36
09/06/2010 01:47:36
09/06/2010 01:47:36
09/06/2010 01:47:41
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ ( for i in *.txt; do
leta "$i"; done) | head -60
Cookie File: john s@accounts[1].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
google.com/accounts/ __utma 173272373.1986555424.1283701346.1283701346.1283701346.1
09/06/2010 01:42:56 09/05/2012 01:42:56 1600
google.com/accounts/ __utmb 173272373.2.10.1283701346 09/06/2010 01:42:56 09/06/2010 02:12:56
1600
google.com/accounts/ __utmz
173272373.1283701346.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none) 09/06/2010 01:42:25
03/07/2011 14:42:25 1600
Cookie File: john s@actnow.com[1].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
actnow.com.au/ __utma 111965844.1463720987.1283701116.1283701116.1283701116.1
09/06/2010 01:38:35 09/05/2012 01:38:35 1600
actnow.com.au/ __utmb 111965844 09/06/2010 01:38:35 09/06/2010 02:08:35 1600
actnow.com.au/ __utmz 111965844.1283701116.1.1.utmccn=(direct)|utmcsr=(direct)|utmcmd=(none)
09/06/2010 01:38:35 03/07/2011 14:38:35 1600
Cookie File: john s@addthis[2].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
addthis.com/ uid 4c83b8ad28cf633f 09/06/2010 01:35:09 10/04/2028 14:19:53 1104
addthis.com/ psc 1 09/06/2010 01:35:09 10/04/2028 14:19:53 1104
Cookie File: john s@adsfac[2].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
```

```
adsfac.net/ FSLIT019105236 uid=998758 09/06/2010 01:03:29 09/07/2010 01:03:32 1024
adsfac.net/ FSLIT019
pctl=105236&pctm=1&fpt=0%2C105236%2C&pct%5Fdate=3901&FL105236=1&FM174560=1&pctc=174560&FQ=1
09/06/2010 01:03:29 10/06/2010 01:03:32 1024
Cookie File: john s@aic.gov[2].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
aic.gov.au/ __utma 32376110.527197245.1283701059.1283701059.1283701059.1 09/06/2010 01:38:24
09/05/2012 01:38:24 1600
aic.gov.au/ __utmb 32376110.3.10.1283701059 09/06/2010 01:38:24 09/06/2010 02:08:24 1600
aic.gov.au/ __utmz 32376110.1283701059.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)
09/06/2010 01:37:38 03/07/2011 14:37:38 1600
Cookie File: john s@antislavery.org[2].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
antislavery.org.au/ __utma 128530012.689650624.1283701134.1283701134.1283701134.1
09/06/2010 01:38:54 09/05/2012 01:38:54 1088
antislavery.org.au/ __utmb 128530012.1.10.1283701134 09/06/2010 01:38:54 09/06/2010 02:08:54
1088
antislavery.org.au/ __utmz 128530012.1283701134.1.1.utm-
csr=actnow.com.au|utmccn=(referral)|utmcmd=referral|utmcct=/Issues/Human_trafficking.aspx
09/06/2010 01:38:54 03/07/2011 14:38:54 1088
Cookie File: john s@atdmt[1].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
atdmt.com/ AA002 1283699010-322478 09/06/2010 01:03:28 09/04/2012 10:00:00 1024
atdmt.com/ MUID DD4E113D243B42D29FA47DAA9FE2E189 09/06/2010 01:03:28 03/24/2011 11:00:00 1024
Cookie File: john s@bangkokairportonline[1].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
bangkokairportonline.com/ __utma 40974257.1625638044.1283700670.1283700670.1283700670.1
09/06/2010 01:33:46 09/05/2012 01:33:46 1600
bangkokairportonline.com/ __utmb 40974257.24.10.1283700670 09/06/2010 01:33:46
09/06/2010 02:03:46 1600
bangkokairportonline.com/ __utmz
40974257.1283700670.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none) 09/06/2010 01:31:10
03/07/2011 14:31:10 1600
Cookie File: john s@bangkokpost[1].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
bangkokpost.com/ _uid62518 70F4D739.1 09/06/2010 01:40:38 01/18/2038 11:00:00 1600
bangkokpost.com/ _ctout62518 1 09/06/2010 01:41:12 09/06/2010 02:01:12 1600
bangkokpost.com/ visit_time 9 09/06/2010 01:41:21 09/09/2010 01:41:21 1600
Cookie File: john s@bigpondsitehelp[2].txt
SITE VARIABLE VALUE CREATION TIME EXPIRE TIME FLAGS
bigpondsitehelp.com/ s_nr 1283701138489 09/06/2010 01:38:58 10/06/2010 02:38:58 1600
bigpondsitehelp.com/ gpv_e48 BP%3ADNS%20Error%20Page 09/06/2010 01:38:58 09/06/2010 02:08:58
1600
bigpondsitehelp.com/ gpv_p43 BP%3ADNS%20Error%20Page 09/06/2010 01:38:58 09/06/2010 02:08:58
1600
bigpondsitehelp.com/ gpv_p49 DNS%20Error%20Page 09/06/2010 01:38:58 09/06/2010 02:08:58 1600
bigpondsitehelp.com/ gpv_e44 DNS%20Error%20Page 09/06/2010 01:38:58 09/06/2010 02:08:58 1600
Cookie File: john s@bs.serving-sys[2].txt
]0;dleigh@alphonse: /mnt/John S/Cookies[01;32mdleigh@alphonse[00m:[01;34m/mnt/John S/Cookies[00m$ exit
exit
Script done on Sun 17 Oct 2010 16:49:21 EST
```

D.12 Sorter

```
Script started on Sat 16 Oct 2010 17:49:43 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  mkdir sorted_files
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cat /home/dleigh/user.sorter.con
category text        ASCII(.*?)text
ext         css,axd,htm,html,php         ASCII(.*?)text
ext         css,axd,htm,html,php         UTF-8 Unicode(.*?)text
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ sorter -
d sorted_files -s -c /home/dleigh/user.sorter.conf disk-part2.img
Analyzing  "disk-part2.img"
  Loading Allocated File Listing
  Processing 1932 Allocated Files and Directories
  100%
All files have been saved to: sorted_files
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ chmod a-
w [1@-[1@R[1@ [C[C[C[C*
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cat sorted_files/mismatch.txt
John S/Favorites/http--headsteadi.com-wp-content-uploads-2008-04-
replica_state_license_plate.gif.url
```

```
  ASCII text, with CRLF line terminators  (Ext: url)
  Image: disk-part2.img  Inode: 2188
  Saved to: text/disk-part2.img-2188.url
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/icon_ticker[1].jpg
  GIF image data, version 89a, 101 x 22  (Ext: jpg)
  Image: disk-part2.img  Inode: 41366
  Saved to: images/disk-part2.img-41366.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/GRedirect[2].aspx
  ASCII text, with very long lines  (Ext: aspx)
  Image: disk-part2.img  Inode: 41371
  Saved to: text/disk-part2.img-41371.aspx
John S/Local Settings/Temporary Inter-
net Files/Content.IE5/SP6FOLM3/CAOH834N.aspx&fu=0&ifi=1&dtd=78
  ASCII text, with very long lines  (Ext: aspx&fu=0&ifi=1&dtd=78)
  Image: disk-part2.img  Inode: 157955
  Saved to: text/disk-part2.img-157955.aspx&fu=0&ifi=1&dtd=78
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/btn_flightInfo[1].gif
  JPEG image data, JFIF standard 1.02  (Ext: gif)
  Image: disk-part2.img  Inode: 179066
  Saved to: images/disk-part2.img-179066.gif
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/CA5W1G5H.jpg
  GIF image data, version 89a, 14 x 17  (Ext: jpg)
  Image: disk-part2.img  Inode: 190518
  Saved to: images/disk-part2.img-190518.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/CAAVCPIT.jpg
  GIF image data, version 89a, 14 x 17  (Ext: jpg)
  Image: disk-part2.img  Inode: 202915
  Saved to: images/disk-part2.img-202915.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/SP6FOLM3/geo[1].aspx
  ASCII text, with no line terminators  (Ext: aspx)
  Image: disk-part2.img  Inode: 210971
  Saved to: text/disk-part2.img-210971.aspx
John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/CAJ8H5N4.ad
  ASCII text, with very long lines  (Ext: ad)
  Image: disk-part2.img  Inode: 307870
  Saved to: text/disk-part2.img-307870.ad
John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/CAJLDV1Z.jpg
  GIF image data, version 89a, 14 x 17  (Ext: jpg)
  Image: disk-part2.img  Inode: 336465
  Saved to: images/disk-part2.img-336465.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/ScriptResource[2].axd
  Lisp/Scheme program text  (Ext: axd)
  Image: disk-part2.img  Inode: 389848
  Saved to: text/disk-part2.img-389848.axd
John S/Local Settings/Temporary Internet Files/Content.IE5/G92JOPQV/fbshare[2].php
  HTML document text (gzip compressed data, from Unix)  (Ext: php)
  Image: disk-part2.img  Inode: 443793
  Saved to: text/disk-part2.img-443793.php
John S/Local Settings/Temporary Inter-
net Files/Content.IE5/G92JOPQV/CAPKCV5H.aspx&fu=0&ifi=1&dtd=10
  ASCII text, with very long lines  (Ext: aspx&fu=0&ifi=1&dtd=10)
  Image: disk-part2.img  Inode: 513829
  Saved to: text/disk-part2.img-513829.aspx&fu=0&ifi=1&dtd=10
John S/Local Settings/Temporary Internet Files/Content.IE5/G92JOPQV/fbshare[1].php
  HTML document text (gzip compressed data, from Unix)  (Ext: php)
  Image: disk-part2.img  Inode: 527444
  Saved to: text/disk-part2.img-527444.php
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/GRedirect[2].aspx
  ASCII text, with very long lines  (Ext: aspx)
  Image: disk-part2.img  Inode: 595506
  Saved to: text/disk-part2.img-595506.aspx
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/CAZE8VZT.jpg
  GIF image data, version 89a, 14 x 17  (Ext: jpg)
  Image: disk-part2.img  Inode: 642652
  Saved to: images/disk-part2.img-642652.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/goggen[1].jpg
  GIF image data, version 89a, 14 x 17  (Ext: jpg)
  Image: disk-part2.img  Inode: 645117
  Saved to: images/disk-part2.img-645117.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/iepngfix[1].htc
  ASCII C++ program text, with CRLF line terminators  (Ext: htc)
  Image: disk-part2.img  Inode: 655059
  Saved to: text/disk-part2.img-655059.htc
```

```
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/CAABO9GP.0
  ASCII text, with very long lines, with no line terminators  (Ext: 0)
  Image: disk-part2.img  Inode: 683444
  Saved to: text/disk-part2.img-683444.0
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/GRedirect[1].aspx
  ASCII text, with very long lines  (Ext: aspx)
  Image: disk-part2.img  Inode: 690375
  Saved to: text/disk-part2.img-690375.aspx
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/ninemsn.com[1]
  HTML document text (gzip compressed data, from Unix)  (Ext: com[1z)
  Image: disk-part2.img  Inode: 720938
  Saved to: text/disk-part2.img-720938.com[1z
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/et4054lc[1].png
  GIF image data, version 89a, 13 x 62  (Ext: png)
  Image: disk-part2.img  Inode: 731758
  Saved to: images/disk-part2.img-731758.png
John S/Local Settings/Temporary Internet Files/Content.IE5/K56JOP2V/CATFRP7T.0
  ASCII text, with very long lines, with no line terminators  (Ext: 0)
  Image: disk-part2.img  Inode: 744329
  Saved to: text/disk-part2.img-744329.0
John S/Local Settings/Application Data/Microsoft/Windows Media/9.0/WMSDKNS.XML
  UTF-8 Unicode (with BOM) HTML document text, with CRLF line terminators  (Ext: xml)
  Image: disk-part2.img  Inode: 810933
  Saved to: text/disk-part2.img-810933.xml
John S/Local Settings/Application Data/Microsoft/Windows Media/9.0/WMSDKNSD.XML
  ASCII text, with CRLF line terminators  (Ext: xml)
  Image: disk-part2.img  Inode: 810935
  Saved to: text/disk-part2.img-810935.xml
John S/Application Data/Microsoft/Internet Explorer/brndlog.bak
  ASCII text, with CRLF line terminators  (Ext: bak)
  Image: disk-part2.img  Inode: 932808
  Saved to: text/disk-part2.img-932808.bak
John S/Application Data/Microsoft/Internet Explorer/Quick Launch/Show Desktop.scf
  ASCII text, with CRLF line terminators  (Ext: scf)
  Image: disk-part2.img  Inode: 933271
  Saved to: text/disk-part2.img-933271.scf
John S/Templates/lotus.wk4
  Lotus 1-2-3 wk4 document data  (Ext: wk4)
  Image: disk-part2.img  Inode: 933654
  Saved to: documents/disk-part2.img-933654.wk4
John S/Templates/amipro.sam
  ASCII text, with CRLF line terminators  (Ext: sam)
  Image: disk-part2.img  Inode: 933656
  Saved to: text/disk-part2.img-933656.sam
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cd sorted_files/
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ feh im
part2.img-41366.jpg images/disk-part2.img-179 066.gif images/disk-part2.img-
190518.jpg images/disk-part2.img-202915.jpg images/disk-part2.img-336465.jp g images/disk-
part2.img-642652.jpg images/disk-part2.img-645117.jpg images/disk-part2.img-731758.png
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ exit
exit
Script done on Sat 16 Oct 2010 17:51:54 EST
Script started on Sat 16 Oct 2010 18:13:03 EST
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ cat so
Images
- disk-part2.img
Files (1932)
Files Skipped (84)
- Non-Files (84)
- 'ignore' category (0)
Extensions
- Extension Mismatches (29)
Categories (1848)
- archive (3)
- audio (1)
- compress (13)
- crypto (0)
- data (14)
- disk (0)
- documents (19)
- exec (0)
- images (981)
- system (11)
```

```
- text (621)
- unknown (185)
- video (0)
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ exit
exit
Script done on Sat 16 Oct 2010 18:13:08 EST
```

D.13 Unallocated and Slack space

```
Script started on Sat 16 Oct 2010 19:49:33 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ blkls -
s disk-part2.img > disk-part2.slack
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ blkls -
A disk-part2.img > disk-part2.unalloc
Error reading image file (tsk_fs_read_block: Address missing in partial im-
age: 204800)) (fatfs_block_walk: block: 204800)
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -Tvdo disk-part2.unalloc.carve disk-part2.unalloc
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Sat Oct 16 19:49:51 2010
Invocation: foremost -Tvdo disk-part2.unalloc.carve disk-part2.unalloc
Output directory: /var/evidence/disk-part2.unalloc.carve_Sat_Oct_16_19_49_51_2010
Configuration file: /etc/foremost.conf
Processing: disk-part2.unalloc
|------------------------------------------------------------------
File: disk-part2.unalloc
Start: Sat Oct 16 19:49:51 2010
Length: 69 MB (72715776 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
*|
Finish: Sat Oct 16 19:49:59 2010
0 FILES EXTRACTED
------------------------------------------------------------------
Foremost finished at Sat Oct 16 19:49:59 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -dTvao disk-part2.slack.carve disk-part2.slack
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Sat Oct 16 19:50:03 2010
Invocation: foremost -dTvao disk-part2.slack.carve disk-part2.slack
Output directory: /var/evidence/disk-part2.slack.carve_Sat_Oct_16_19_50_03_2010
Configuration file: /etc/foremost.conf
Processing: disk-part2.slack
|------------------------------------------------------------------
File: disk-part2.slack
Start: Sat Oct 16 19:50:03 2010
Length: 919 KB (941056 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
*|
Finish: Sat Oct 16 19:50:03 2010
0 FILES EXTRACTED
------------------------------------------------------------------
Foremost finished at Sat Oct 16 19:50:03 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ hd disk-
part2.slack
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000e5200  28 23 2c 23 23 30 5c 29  1e 04 1a 00 01 06 17 23  |(#,##0\).......#|
000e5210  2c 23 23 30 2e 30 30 5f  29 3b 5c 28 23 2c 23 23  |,##0.00_);\(#,##|
000e5220  30 2e 30 30 5c 29 1e 04  1f 00 01 07 1c 23 2c 23  |0.00\).......#,#|
000e5230  23 30 2e 30 30 5f 29 3b  5b 52 65 64 5d 5c 28 23  |#0.00_);[Red]\(#|
000e5240  2c 23 23 30 2e 30 30 5c  29 1e 04 1a 00 02 00 17  |,##0.00\).......|
000e5250  22 24 22 23 2c 23 23 30  5f 29 3b 5c 28 22 24 22  |"$"#,##0_);\("$"|
000e5260  23 2c 23 23 30 5c 29 1e  04 1f 00 02 01 1c 22 24  |#,##0\)."......"$|
000e5270  22 23 2c 23 23 30 5f 29  3b 5b 52 65 64 5d 5c 28  |"#,##0_);[Red]\(|
000e5280  22 24 22 23 2c 23 23 30  5c 29 1e 04 20 00 02 02  |"$"#,##0\).. ...|
000e5290  1d 22 24 22 23 2c 23 23  30 2e 30 30 5f 29 3b 5c  |."$"#,##0.00_);\|
000e52a0  28 22 24 22 23 2c 23 23  30 2e 30 30 5c 29 1e 04  |("$"#,##0.00\)..|
000e52b0  25 00 02 03 22 22 24 22  23 2c 23 23 30 2e 30 30  |%..""$"#,##0.00|
```

```
000e52c0  5f 29 3b 5b 52 65 64 5d  5c 28 22 24 22 23 2c 23  |_);[Red]\("$"#,#|
000e52d0  23 30 2e 30 30 5c 29 1e  04 05 00 05 00 02 30 25  |#0.00\).......0%|
000e52e0  1e 04 08 00 05 01 05 30  2e 30 30 25 1e 04 0b 00  |.......0.00%....|
000e52f0  07 00 08 30 2e 30 30 45  2b 30 30 1e 04 09 00 06  |...0.00E+00.....|
000e5300  00 06 23 5c 20 3f 2f 3f  1e 04 0b 00 06 01 08 23  |..#\ ?/?.......#|
000e5310  5c 20 3f 3f 2f 3f 3f 1e  04 09 00 03 00 06 6d 2f  |\ ??/??.......m/|
000e5320  64 2f 79 79 1e 04 0d 00  03 01 0a 64 5c 2d 6d 6d  |d/yy.......d\-mm|
000e5330  6d 5c 2d 79 79 1e 04 09  00 03 02 06 64 5c 2d 6d  |m\-yy.......d\-m|
000e5340  6d 6d 1e 04 0a 00 03 03  07 6d 6d 6d 5c 2d 79 79  |mm.......mmm\-yy|
000e5350  1e 04 0e 00 04 00 0b 68  3a 6d 6d 5c 20 41 4d 2f  |.......h:mm\ AM/|
000e5360  50 4d 1e 04 11 00 04 01  0e 68 3a 6d 6d 3a 73 73  |PM.......h:mm:ss|
000e5370  5c 20 41 4d 2f 50 4d 1e  04 07 00 04 02 04 68 3a  |\ AM/PM.......h:|
000e5380  6d 6d 1e 04 0a 00 04 03  07 68 3a 6d 6d 3a 73 73  |mm.......h:mm:ss|
000e5390  1e 04 0f 00 04 04 0c 6d  2f 64 2f 79 79 5c 20 68  |.......m/d/yy\ h|
000e53a0  3a 6d 6d 18 02 07 00 20  00 0c 01 00 00 05 18 02  |:mm.... ........|
000e53b0  07 00 20 00 0c 01 00 00  09 18 02 07 00 20 00 0c  |.. .......... ..|
000e53c0  01 00 00 04 18 02 07 00  20 00 0c 01 00 00 06 18  |........ .......|
000e53d0  02 07 00 20 00 0c 01 00  00 07 18 02 07 00 20 00  |... .......... .|
000e53e0  0c 01 00 00 08 12 00 02  00 00 00 19 00 02 00 00  |................|
000e53f0  00 63 00 02 00 00 00 13  00 02 00 00 00 43 04 0c  |.c...........C..|
000e5400  00 00 00 f5 ff 20 00 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5410  00 01 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e5430  00 02 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e5450  00 00 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e54f0  00 00 00 01 00 20 00 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5500  00 05 08 f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5510  00 05 06 f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5520  00 05 0c f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5530  00 05 0a f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5540  00 05 0d f5 ff 20 f8 00  ce 00 00 00 00 93 02 04  |..... ..........|
000e5550  00 10 80 03 ff 93 02 04  00 11 80 06 ff 93 02 04  |................|
000e5560  00 12 80 04 ff 93 02 04  00 13 80 07 ff 93 02 04  |................|
000e5570  00 00 80 00 ff 93 02 04  00 14 80 05 ff 55 00 02  |.............U..|
000e5580  00 08 00 00 02 0a 00 00  00 00 00 00 00 00 01 00  |................|
000e5590  00 3d 00 0a 00 78 00 4b  00 2e 3b 08 25 00 00 3e  |.=...x.K..;.%..>|
000e55a0  02 0a 00 b6 00 00 00 00  00 00 00 00 00 1d 00 0f  |................|
000e55b0  00 03 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000e55c0  94 00 00 00 ab 00 22 00  20 00 ff ff ff ff ff ff  |......". .......|
000e55d0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000e55e0  ff ff ff ff ff ff ff ff  ff ff 0a 00 00 00 00 00  |................|
000e55f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000e5600  09 04 06 00 00 00 10 00  4e 08 5c 00 20 00 01 2e  |........N.\. ...|
000e5610  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20  |                |
000e5620  20 20 20 20 20 20 20 20  20 20 20 20 20 20 0b 02  |              ..|
000e5630  0c 00 a3 03 00 00 00 00  00 00 fd 03 00 00 42 00  |..............B.|
000e5640  02 00 e4 04 0c 00 02 00  64 00 0d 00 02 00 01 00  |........d.......|
000e5650  0e 00 02 00 01 00 0f 00  02 00 01 00 10 00 08 00  |................|
000e5660  fc a9 f1 d2 4d 62 50 3f  11 00 02 00 00 00 22 00  |....MbP?......".|
000e5670  02 00 00 00 2a 00 02 00  00 00 2b 00 02 00 01 00  |....*.....+.....|
000e5680  5f 00 02 00 01 00 82 00  02 00 00 00 80 00 08 00  |_...............|
000e5690  00 00 00 00 00 00 00 00  25 02 04 00 00 00 ff 00  |........%.......|
000e56a0  8c 00 04 00 01 00 01 00  8d 00 02 00 00 00 81 00  |................|
000e56b0  02 00 c1 04 31 02 14 00  c8 00 00 00 ff 7f 0d 4d  |....1..........M|
000e56c0  53 20 53 61 6e 73 20 53  65 72 69 66 31 02 14 00  |S Sans Serif1...|
000e56d0  c8 00 01 00 ff 7f 0d 4d  53 20 53 61 6e 73 20 53  |.......MS Sans S|
000e56e0  65 72 69 66 31 02 14 00  c8 00 02 00 ff 7f 0d 4d  |erif1..........M|
000e56f0  53 20 53 61 6e 73 20 53  65 72 69 66 31 02 14 00  |S Sans Serif1...|
000e5700  c8 00 03 00 ff 7f 0d 4d  53 20 53 61 6e 73 20 53  |.......MS Sans S|
000e5710  65 72 69 66 31 02 14 00  c8 00 00 00 ff 7f 0d 4d  |erif1..........M|
000e5720  53 20 53 61 6e 73 20 53  65 72 69 66 14 00 03 00  |S Sans Serif....|
000e5730  02 26 46 15 00 08 00 07  50 61 67 65 20 26 50 83  |.&F.....Page &P.|
000e5740  00 02 00 00 00 84 00 02  00 00 00 26 00 08 00 00  |...........&....|
000e5750  00 00 00 00 00 e8 3f 27  00 08 00 00 00 00 00 00  |......?'........|
000e5760  00 e8 3f 28 00 08 00 00  00 00 00 00 f0 3f 29  |..?(..........?)|
000e5770  00 08 00 00 00 00 00 00  00 f0 3f a1 00 0c 00 c1  |..........?.....|
000e5780  04 01 00 01 00 01 00 01  00 04 00 40 00 02 00 00  |...........@....|
000e5790  00 56 00 02 00 1b 00 1e  04 0a 00 00 00 07 47 65  |.V............Ge|
000e57a0  6e 65 72 61 6c 1e 04 04  00 01 00 01 30 1e 04 07  |neral.......0...|
000e57b0  00 01 01 04 30 2e 30 30  1e 04 08 00 01 02 05 23  |....0.00.......#|
000e57c0  2c 23 23 30 1e 04 0b 00  01 03 08 23 2c 23 23 30  |,##0.......#,##0|
```

```
000e57d0  2e 30 30 1e 04 14 00 01  04 11 23 2c 23 23 30 5f  |.00.......#,##0_|
000e57e0  29 3b 5c 28 23 2c 23 23  30 5c 29 1e 04 19 00 01  |);\(#,##0\).....|
000e57f0  05 16 23 2c 23 23 30 5f  29 3b 5b 52 65 64 5d 5c  |..#,##0_);[Red]\|
000e5800  28 23 2c 23 23 30 5c 29  1e 04 1a 00 01 06 17 23  |(#,##0\).......#|
000e5810  2c 23 23 30 2e 30 30 5f  29 3b 5c 28 23 2c 23 23  |,##0.00_);\(#,##|
000e5820  30 2e 30 30 5c 29 1e 04  1f 00 01 07 1c 23 2c 23  |0.00\).......#,#|
000e5830  23 30 2e 30 30 5f 29 3b  5b 52 65 64 5d 5c 28 23  |#0.00_);[Red]\(#|
000e5840  2c 23 23 30 2e 30 30 5c  29 1e 04 1a 00 02 00 17  |,##0.00\).......|
000e5850  22 24 22 23 2c 23 23 30  5f 29 3b 5c 28 22 24 22  |"$"#,##0_);\("$"|
000e5860  23 2c 23 23 30 5c 29 1e  04 1f 00 02 01 1c 22 24  |#,##0\)."$|
000e5870  22 23 2c 23 23 30 5f 29  3b 5b 52 65 64 5d 5c 28  |"#,##0_);[Red]\(|
000e5880  22 24 22 23 2c 23 23 30  5c 29 1e 04 20 00 02 02  |"$"#,##0\).. ...|
000e5890  1d 22 24 22 23 2c 23 23  30 2e 30 30 5f 29 3b 5c  |."$"#,##0.00_);\|
000e58a0  28 22 24 22 23 2c 23 23  30 2e 30 30 5c 29 1e 04  |("$"#,##0.00\)..|
000e58b0  25 00 02 03 22 22 24 22  23 2c 23 23 30 2e 30 30  |%..""$"#,##0.00|
000e58c0  5f 29 3b 5b 52 65 64 5d  5c 28 22 24 22 23 2c 23  |_);[Red]\("$"#,#|
000e58d0  23 30 2e 30 30 5c 29 1e  04 05 00 05 00 02 30 25  |#0.00\).......0%|
000e58e0  1e 04 08 00 05 01 05 30  2e 30 30 25 1e 04 0b 00  |.......0.00%....|
000e58f0  07 00 08 30 2e 30 30 45  2b 30 30 1e 04 09 00 06  |...0.00E+00.....|
000e5900  00 06 23 5c 20 3f 2f 3f  1e 04 0b 00 06 01 08 23  |..#\ ?/?.......#|
000e5910  5c 20 3f 3f 2f 3f 3f 1e  04 09 00 03 00 06 6d 2f  |\ ??/??......m/|
000e5920  64 2f 79 79 1e 04 0d 00  03 01 0a 64 5c 2d 6d 6d  |d/yy.......d\-mm|
000e5930  6d 5c 2d 79 79 1e 04 09  00 03 02 06 64 5c 2d 6d  |m\-yy.......d\-m|
000e5940  6d 6d 1e 04 0a 00 03 03  07 6d 6d 6d 5c 2d 79 79  |mm.......mmm\-yy|
000e5950  1e 04 0e 00 04 00 0b 68  3a 6d 6d 5c 20 41 4d 2f  |.......h:mm\ AM/|
000e5960  50 4d 1e 04 11 00 04 01  0e 68 3a 6d 6d 3a 73 73  |PM.......h:mm:ss|
000e5970  5c 20 41 4d 2f 50 4d 1e  04 07 00 04 02 04 68 3a  |\ AM/PM.......h:|
000e5980  6d 6d 1e 04 0a 00 04 03  07 68 3a 6d 6d 3a 73 73  |mm.......h:mm:ss|
000e5990  1e 04 0f 00 04 04 0c 6d  2f 64 2f 79 79 5c 20 68  |.......m/d/yy\ h|
000e59a0  3a 6d 6d 18 02 07 00 20  00 0c 01 00 00 05 18 02  |:mm.... ........|
000e59b0  07 00 20 00 0c 01 00 00  09 18 02 07 00 20 00 0c  |.. .......... ..|
000e59c0  01 00 00 04 18 02 07 00  20 00 0c 01 00 00 06 18  |........ .......|
000e59d0  02 07 00 20 00 0c 01 00  00 07 18 02 07 00 20 00  |... .......... .|
000e59e0  0c 01 00 00 08 12 00 02  00 00 00 19 00 02 00 00  |................|
000e59f0  00 63 00 02 00 00 00 13  00 02 00 00 00 43 04 0c  |.c...........C..|
000e5a00  00 00 00 f5 ff 20 00 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5a10  00 01 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e5a30  00 02 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e5a50  00 00 00 f5 ff 20 f4 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
*
000e5af0  00 00 00 01 00 20 00 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5b00  00 05 08 f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5b10  00 05 06 f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5b20  00 05 0c f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5b30  00 05 0a f5 ff 20 f8 00  ce 00 00 00 00 43 04 0c  |..... .......C..|
000e5b40  00 05 0d f5 ff 20 f8 00  ce 00 00 00 00 93 02 04  |..... ..........|
000e5b50  00 10 80 03 ff 93 02 04  00 11 80 06 ff 93 02 04  |................|
000e5b60  00 12 80 04 ff 93 02 04  00 13 80 07 ff 93 02 04  |................|
000e5b70  00 00 80 00 ff 93 02 04  00 14 80 05 ff 55 00 02  |.............U..|
000e5b80  00 08 00 00 02 0a 00 00  00 00 00 00 00 00 01 00  |................|
000e5b90  00 3d 00 0a 00 78 00 4b  00 2e 3b 08 25 00 00 3e  |.=...x.K..;.%..>|
000e5ba0  02 0a 00 b6 00 00 00 00  00 00 00 00 00 1d 00 0f  |................|
000e5bb0  00 03 00 00 00 00 00 00  01 00 00 00 00 00 00 00  |................|
000e5bc0  94 00 00 00 ab 00 22 00  20 00 ff ff ff ff ff ff  |......". .......|
000e5bd0  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
000e5be0  ff ff ff ff ff ff ff ff  ff ff 0a 00 00 00 00 00  |................|
000e5bf0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000e5c00
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  hd disk-
part2.unalloc
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
04558e00
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sat 16 Oct 2010 19:50:34 EST
```

D.14 File carving of FAT32 and entire disk image

```
Script started on Sun 17 Oct 2010 02:00:30 EST
```

```
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -Tdo disk-image.img.carve disk-image.img
Processing: disk-image.img
|**|
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ fore-
most -Tdo disk-part2.img.carve disk-part2.img
Processing: disk-part2.img
|*|
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ head -
20 disk-*carve*/audit.txt
==> disk-image.img.carve_Sun_Oct_17_02_00_57_2010/audit.txt <==
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Sun Oct 17 02:00:57 2010
Invocation: foremost -Tdo disk-image.img.carve disk-image.img
Output directory: /var/evidence/disk-image.img.carve_Sun_Oct_17_02_00_57_2010
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: disk-image.img
Start: Sun Oct 17 02:00:57 2010
Length: 130 MB (136314880 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
0:  00027899.jpg         2 KB     14284288
1:  00027906.jpg        12 KB     14287872
2:  00027931.jpg         2 KB     14300672
3:  00027942.jpg        12 KB     14306304
4:  00028251.jpg         3 KB     14464512
5:  00028296.jpg         6 KB     14487552
==> disk-part2.img.carve_Sun_Oct_17_02_01_30_2010/audit.txt <==
Foremost version 1.5.6 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
Foremost started at Sun Oct 17 02:01:30 2010
Invocation: foremost -Tdo disk-part2.img.carve disk-part2.img
Output directory: /var/evidence/disk-part2.img.carve_Sun_Oct_17_02_01_30_2010
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: disk-part2.img
Start: Sun Oct 17 02:01:30 2010
Length: 100 MB (104857600 bytes)

Num  Name (bs=512)        Size  File Offset  Comment
0:  00007419.jpg         2 KB      3798528
1:  00007426.jpg        12 KB      3802112
2:  00007451.jpg         2 KB      3814912
3:  00007462.jpg        12 KB      3820544
4:  00007771.jpg         3 KB      3978752
5:  00007816.jpg         6 KB      4001792
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ head -
20 disk-*carve*/audit.txt[C[C[C[C[1P[1P[1P[1P[1@t[1@a[1@i[1@l[C[1@ [C[C[1P[C[C[C[1P disk-
*carve*/audit.txt5 disk-*carve*/audit.txt
tail: option used in invalid context -- 2
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ tail -
25 disk-*carve*/audit.txt[C[C[C[C[C[1@n[1@
==> disk-image.img.carve_Sun_Oct_17_02_00_57_2010/audit.txt <==
1244:  00069923.png        528 B     35800576    (16 x 16)
1245:  00069942.png        313 B     35810304    (52 x 54)
1246:  00070266.png         2 KB     35976192    (28 x 1323)
1247:  00070275.png        114 B     35980800    (8 x 8)
1248:  00070277.png        628 B     35981824    (18 x 20)
1249:  00070415.png         2 KB     36052480    (83 x 30)
1250:  00070420.png        694 B     36055040    (22 x 22)
1251:  00071004.png         3 KB     36354048    (111 x 56)
1252:  00071640.png        331 B     36679680    (14 x 14)
1253:  00225397.jpg         45 KB    115403264
1254:  00225488.rar         2 KB     115449868   Password Protected:
Finish: Sun Oct 17 02:01:13 2010
1255 FILES EXTRACTED
jpg:= 360
gif:= 622
rif:= 1
htm:= 128
ole:= 4
```

```
rar:= 1
png:= 139
-----------------------------------------------------------------
Foremost finished at Sun Oct 17 02:01:13 2010
==> disk-part2.img.carve_Sun_Oct_17_02_01_30_2010/audit.txt <==
1241:  00048555.png        670 B     24860160    (236 x 270)
1242:  00049274.png        914 B     25228288    (960 x 85)
1243:  00049366.png        169 B     25275392    (1 x 50)
1244:  00049443.png        528 B     25314816    (16 x 16)
1245:  00049462.png        313 B     25324544    (52 x 54)
1246:  00049786.png         2 KB     25490432    (28 x 1323)
1247:  00049795.png        114 B     25495040    (8 x 8)
1248:  00049797.png        628 B     25496064    (18 x 20)
1249:  00049935.png         2 KB     25566720    (83 x 30)
1250:  00049940.png        694 B     25569280    (22 x 22)
1251:  00050524.png         3 KB     25868288    (111 x 56)
1252:  00051160.png        331 B     26193920    (14 x 14)
Finish: Sun Oct 17 02:01:43 2010
1253 FILES EXTRACTED
jpg:= 359
gif:= 622
rif:= 1
htm:= 128
ole:= 4
png:= 139
-----------------------------------------------------------------
Foremost finished at Sun Oct 17 02:01:43 2010
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sun 17 Oct 2010 02:02:31 EST
```

D.15 MACtime analysis

```
Script started on Sun 17 Oct 2010 02:36:04 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  fls -r -
m ■ disk-part2.img > disk-part2.mactimes
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ head disk-
part2.mactimes
0|/John S|4|d/drwxrwxrwx|0|0|1536|1355230800|1355271120|0|1283926016
0|/John S/Recent|22|d/drwxrwxrwx|0|0|512|1355230800|1355271120|0|1283926016
0|/John S/Recent/replica_state_license_plate.gif.lnk|40|r/rrwxrwxrwx|0|0|503|1355230800|1355271120|0|1283926016
0|/John S/Recent/Desktop.ini|42|r/rrwxrwxrwx|0|0|150|1355230800|1355271120|0|1283926016
0|/John S/Recent/Links.txt.lnk|44|r/rrwxrwxrwx|0|0|530|1355230800|1355271120|0|1283926016
0|/John S/Recent/transfer on rohit-
laptop server (Samba, Ubuntu) (10.0.0.2).lnk|50|r/rrwxrwxrwx|0|0|493|1355230800|1355271120|0|1283926016
0|/John S/ntuser.ini|24|r/rrwxrwxrwx|0|0|178|1355230800|1355271120|0|1283926016
0|/John S/My Documents|26|d/drwxrwxrwx|0|0|512|1355230800|1355271120|0|1283926016
0|/John S/My Documents/My Music|150|d/drwxrwxrwx|0|0|512|1355230800|1355271120|0|1283926016
0|/John S/My Documents/My Music/Sample Mu-
sic.lnk|167|r/rrwxrwxrwx|0|0|542|1355230800|1355271120|0|1283926016
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ wc disk-
part2.mactimes
  1932   9286 288035 disk-part2.mactimes
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mactime -
b disk-part2.mactimes > disk-part2.mactime.analysis
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ head disk-
part2.mactime.analysis
Thu Jan 01 1970 10:00:00      512 ..c. d/drwxrwxrwx 0        0        150      /John S/My Docu-
ments/My Music
                            57632 ..c. r/rrwxrwxrwx 0        0        154      /John S/My Docu-
ments/replica_state_license_plate.gif
                             3979 ..c. r/rrwxrwxrwx 0        0        154820   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/CA2EE4FT.htm
                              107 ..c. r/rrwxrwxrwx 0        0        154823   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/icon_arrow_grey[1].gif
                            39444 ..c. r/rrwxrwxrwx 0        0        154825   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/s_code[1].js
                            51792 ..c. r/rrwxrwxrwx 0        0        154827   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/arr3[1].jpg
                             3017 ..c. r/rrwxrwxrwx 0        0        154831   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/2345984_com_abs00130[1].jpg
                               77 ..c. r/rrwxrwxrwx 0        0        156      /John S/My Docu-
```

```
ments/desktop.ini
                            5815 ..c. r/rrwxrwxrwx 0        0        157955   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/CAOH834N.aspx&fu=0&ifi=1&dtd=78
                             594 ..c. r/rrwxrwxrwx 0        0        157958   /John S/Local Set-
tings/Temporary Internet Files/Content.IE5/SP6FOLM3/arrow_icon[1].jpg
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ wc disk-
part2.mactime.analysis
   7710   83440 1254719 disk-part2.mactime.analysis
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ mactime -
d -b disk-part2.mactimes > disk-part2.mactime.analysis.csv
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sun 17 Oct 2010 02:36:54 EST
Script started on Sun 17 Oct 2010 03:27:52 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ cut -c1-
24 disk-part2.mactime.analysis.csv | sort | uniq -c
      1 Date,Size,Type,Mode,UID,
   1928 Thu Jan 01 1970 10:00:00
   1926 Wed Dec 12 2012 00:00:00
   1926 Wed Dec 12 2012 11:12:00
      2 Wed Sep 08 2010 00:00:00
      2 Wed Sep 08 2010 15:17:22
    425 Wed Sep 08 2010 16:06:56
    402 Wed Sep 08 2010 16:06:58
    403 Wed Sep 08 2010 16:07:00
    403 Wed Sep 08 2010 16:07:02
    293 Wed Sep 08 2010 16:07:04
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sun 17 Oct 2010 03:29:53 EST
```

D.16 Metadata Analysis

```
Script started on Sat 16 Oct 2010 18:37:03 EST
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$  cd im
ages/
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
jpgcom -verbose $i; done)  >& /tmp/jpeg-comment-output
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
20 /tmp/jpeg-comment-output
disk-part2.img-154823.gif: GIF image data, version 89a, 5 x 8
Not a JPEG file
disk-part2.img-154827.jpg: JPEG image data, JFIF standard 1.01
JPEG image is 600w * 450h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-154831.jpg: JPEG image data, JFIF standard 1.02
JPEG image is 110w * 110h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-154.gif: GIF image data, version 87a, 500 x 335
Not a JPEG file
disk-part2.img-157958.jpg: JPEG image data, JFIF standard 1.02
APP12 contains:
Ducky\000\001\000\004\000\000\000d\000\000
JPEG image is 10w * 10h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-157960.jpg: JPEG image data, JFIF standard 1.02
APP12 contains:
Ducky\000\001\000\004\000\000\000<\000\000
JPEG image is 2000w * 320h, 3 color components, 8 bits per sample
JPEG process: Baseline
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
C 2 comment /tmp/jpeg-comment-output
disk-part2.img-261292.gif: GIF image data, version 89a, 43 x 18
Not a JPEG file
disk-part2.img-262068.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-
jpeg v1.0 (using IJ"
CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
--
JPEG image is 145w * 95h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-286236.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-
jpeg v1.0 (using IJ"
```

```
CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
--
disk-part2.img-427190.gif: GIF image data, version 89a, 191 x 204
Not a JPEG file
disk-part2.img-
427198.jpg: JPEG image data, JFIF standard 1.00, comment: "LEAD Technologies Inc. V1.01"
LEAD Technologies Inc. V1.01\000
JPEG image is 728w * 90h, 3 color components, 8 bits per sample
--
JPEG image is 96w * 68h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-437178.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-
jpeg v1.0 (using IJ"
CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
--
JPEG image is 219w * 73h, 3 color components, 8 bits per sample
JPEG process: Baseline
disk-part2.img-544822.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-
jpeg v1.0 (using IJ"
CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
--
disk-part2.img-744334.gif: GIF image data, version 89a, 1 x 1
Not a JPEG file
disk-part2.img-744337.jpg: JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-
jpeg v1.0 (using IJ"
CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), default quality
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
jpgcom -verbose disk-part2.img-358752.jpg
APP12 contains:
Ducky\000\001\000\004\000\000\000<\000\002\002\242\000\000\001D\000A\000d\000a\000m\000 \000G\000o\000o\000d\000e\000s
JPEG image is 145w * 95h, 3 color components, 8 bits per sample
JPEG process: Baseline
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
jpgcom -verbose disk-part2.img-358752.jpg > /var/evi dence/disk-part2.img-358752.jpg.comment
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
jpgcom -verbose disk-part2.img-436609.jpg
APP12 contains:
Ducky\000\001\000\004\000\000\000+\000\002\005\324\000\000\002\350\000F\000r\000o\000m\000:\000 \000I\000T\000V\000
\000
\000T\000R\000I\000N\000N\000Y\000 \000A\000N\000D\000 \000S\000U\000S\000A\000N\000N\000A\000H\000 \000U\000N\000D\00
\000
\000O\000n\000 \000I\000T\000V\000 \0001\000
\000
\000P\000i\000c\000t\000u\000r\000e\000 \000s\000h\000o\000w\000s\000:\000 \000,\000 \000(\0001\000-
\000r\000)\000 \000 \000S\000u\000s\000a\000n\000n\000a\000h\000 \000a\000n\000d\000 \000T\000r\000i\000n\000n\000y\00
\000
\000I\000T\000V\000 \000P\000i\000c\000t\000u\000r\000e\000 \000c\000o\000n\000t\000a\000c\000t\000 \000-
\000 \000P\000e\000t\000e\000r\000 \000G\000r\000a\000y\000 \000-
\000 \0000\0008\0004\0004\0008\0008\000 \0001\0003\0000\0004\0006\000
\000p\000e\000t\000e\000r\000.\000g\000r\000a\000y\000@\000i\000t\000v\000.\000c\000o\000m\000
\000
\000T\000h\000i\000s\000 \000p\000h\000o\000t\000o\000g\000r\000a\000p\000h\000 \000i\000s\000 \000(\000C\000)\000 \00
\000r\000e\000p\000r\000o\000d\000u\000c\000t\000i\000o\000n\000 \000f\000e\000e\000 \000w\000i\0001\0001\000 \000b\00
\000w\000w\000w\000.\000i\000t\000v\000p\000i\000c\000t\000u\000r\000e\000s\000.\000c\000o\000m\000\000
JPEG image is 96w * 68h, 3 color components, 8 bits per sample
JPEG process: Baseline
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
jpgcom -verbose disk-part2.img-436609.jpg > /var/evi dence/disk-part2.img-436609.jpg.comment
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
C 5 disk-part2.img-436609.jpg ../images.txt
  Saved to: images/disk-part2.img-436606.gif
John S/Local Settings/Temporary Internet Files/Content.IE5/G92JOPQV/trinnysus_th[2].jpg
  JPEG image data, JFIF standard 1.02
  Image: disk-part2.img  Inode: 436609
  Saved to: images/disk-part2.img-436609.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/G92JOPQV/photo2[1].jpg
  JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-jpeg v1.0 (using IJ"
  Image: disk-part2.img  Inode: 437178
  Saved to: images/disk-part2.img-437178.jpg
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
C 5 disk-part2.img-358752.jpg ../images.txt
  Saved to: images/disk-part2.img-358749.gif
John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/100905_swanswin145[1].jpg
```

```
  JPEG image data, JFIF standard 1.02
  Image: disk-part2.img  Inode: 358752
  Saved to: images/disk-part2.img-358752.jpg
John S/Local Settings/Temporary Internet Files/Content.IE5/I9EFGXI7/ft[1].gif
  GIF image data, version 89a, 1 x 1
  Image: disk-part2.img  Inode: 359519
  Saved to: images/disk-part2.img-359519.gif
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
exit
Script done on Sat 16 Oct 2010 18:39:16 EST
Script started on Sat 16 Oct 2010 18:57:01 EST
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
tify -format '%[EXIF:*]' * | head -20
Orientation=1
XResolution=300/1
YResolution=300/1
ResolutionUnit=2
Software=Adobe Photoshop CS Windows
DateTime=2006:07:09 17:50:27
ExifOffset=164
ColorSpace=65535
ExifImageWidth=600
ExifImageLength=502Orientation=1
XResolution=720000/10000
YResolution=720000/10000
ResolutionUnit=2
Software=Adobe Photoshop CS3 Windows
DateTime=2008:12:16 13:21:07
ExifOffset=164
ColorSpace=65535
ExifImageWidth=75
ExifImageLength=17Orientation=1
XResolution=72/1
]0;dleigh@alphonse: /var/evidence/sorted_files/images[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files/imag
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ cd ..
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  iden-
tify -format '%[EXIF:*]' REPLICA_.JPG
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  iden-
tify -format '%[EXIF:*]' REPLICA_.JPG[K[K[K[K[K[K[K[K[K[K[Kreplica_state_license_plate.gif
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sat 16 Oct 2010 18:57:40 EST
Script started on Sat 16 Oct 2010 18:47:44 EST
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$  rdjpg-
com -verbose REPLICA_.JPG
APP12 contains:
Ducky\000\001\000\004\000\000\000\036\000\000
JPEG image is 500w * 335h, 3 color components, 8 bits per sample
JPEG process: Baseline
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ un-
rar l 00000091.rar
UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal
Archive 00000091.rar
 Name             Size   Packed Ratio  Date   Time     Attr      CRC   Meth Ver
-------------------------------------------------------------------------------
*Local.txt        4697     2624  55% 07-09-10 02:18 -rw-r--r-- D0EBF5E4 m3b 2.9
-------------------------------------------------------------------------------
    1             4697     2624  55%
]0;dleigh@alphonse: /var/evidence[01;32mdleigh@alphonse[00m:[01;34m/var/evidence[00m$ exit
exit
Script done on Sat 16 Oct 2010 18:48:22 EST
```

D.17 Text Search

```
Script started on Sun 17 Oct 2010 18:07:10 EST
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep -
i 'smith' */*
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep -
i 'kayak' */*
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep -
i 'links.txt' */*~
grep: */*~: No such file or directory
```

```
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep -
i 'links.txt' */*~[K
Binary file system/disk-part2.img-2460.dat matches
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ file s
part2.img-2460.dat
system/disk-part2.img-2460.dat: MS Windows registry file, NT/2000 or above
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ g[Kgre
C 3 system/disk-part2.img-2460.dat system.txt
John S/NTUSER.DAT
  MS Windows registry file, NT/2000 or above
  Image: disk-part2.img  Inode: 2460
  Saved to: system/disk-part2.img-2460.dat
John S/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat.LOG
  MS Windows registry file, NT/2000 or above
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep -
i 'local.txt' */*
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$  grep
i 'john' */*
documents/disk-part2.img-731760.htm:R G Casey Building, John McEwen Crescent<br />
documents/disk-part2.img-731760.htm:  John McEwen Crescent<br/>
documents/disk-part2.img-731760.htm:  John McEwen Crescent<br/>
Binary file system/disk-part2.img-2460.dat matches
text/disk-part2.img-156.ini:Owner=John S
text/disk-part2.img-169.ini:Owner=John S
text/disk-part2.img-2057.ini:Owner=John S
text/disk-part2.img-
245543:document.write("<IFRAME WIDTH=\"728\" HEIGHT=\"90\" SCROLLING=\"No\" FRAMEBOR-
DER=\"0\" MARGINHEIGHT=\"0\" MARGIN-
WIDTH=\"0\" SRC=\"http://media1.bangkokpost.com/ads/johnnie_walker_728x90_250810.html\"></IFRAME>");
text/disk-part2.img-254172.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-262080.js:/* DOMReady: based on work by: Dean Edwards/John Re-
sig/Matthias Miller/Diego Perini */
text/disk-part2.img-269850.js:     Matthias Miller, Dean Edwards and John Resig. */
text/disk-part2.img-278582.js: * Copyright (c) 2009 John Resig
text/disk-part2.img-288591.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-295897.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-332191.css:   Developed by John Athayde and Justin B. Hankins at Meticulous
text/disk-part2.img-356838.css:/* $Id: ie.css,v 1.1 2008/02/15 16:22:09 johnalbin Exp $ */
text/disk-part2.img-399501.htm:
<span class="odd"><span class="image"><a href="http://video.msn.com/video.aspx?mkt=en-
au&brand=ninemsn&vid=23c49098-a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_NH_NEWS_TAB_VIDEO','1')"><img src="http://images.ninemsn.com.au/resizer.aspx
tor contestants have punch-up" title="9RAW: Rude X Factor contestants have punch-up" bor-
der="0" align="middle"></a></span><span class="title"><a href="http://video.msn.com/video.aspx?mkt=en-
au&brand=ninemsn&vid=23c49098-a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_NH_NEWS_TAB_VIDEO','2')">9RAW: Rude X Factor contes-
tants have punch-up</a></span><span class="text">September 05, 2010: Aspir-
ing singers Abbey Johnston and Lisa Parker have shocked X Factor viewers after insult-
ing some of the judge panel and then get-
ting into a fight with each other on stage.</span></span><span class="even">
text/disk-part2.img-
399501.htm:                    <span class="even" id="item_7" ><span class="image"><a href="http://video.ninemsn.com.a
a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_MSN+video+category','13')"><img src="http://images.ninemsn.com.au/resizer.as
tor contestants have punch-up" title="9RAW: Rude X Factor contestants have punch-up" bor-
der="0" align="middle"></a></span><span class="content"><span class="title"><a href="http://video.ninemsn.com.au/video
a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_MSN+video+category','14')">9RAW: Rude X Factor con-
testants have punch-up</a></span><span class="text">September 05, 2010: Aspir-
ing singers Abbey Johnston and Lisa Parker have shocked X Factor viewers after insult-
ing some of the judge panel and then get-
ting into a fight with each other on stage.</span></span></span>
text/disk-part2.img-414544.js: * Copyright (c) 2009 John Resig
text/disk-part2.img-43259.js: * Copyright (c) 2009 John Resig
text/disk-part2.img-460825.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-470705.htm:
<li><a href='http://www.pattayadailynews.com/en/2010/09/05/justice-for-sale-freedom-for-a-
fee/' title='Justice for Sale, Freedom for a Fee' target='_blank'>Justice for Sale, Free-
dom for a Fee</a></li><li><a href='http://www.pattayadailynews.com/en/2010/09/05/wagner%e2%80%99s-
ring-by-john-l-digaetani/' title='Wagner's Ring by John L. DiGaetani' tar-
get='_blank'>Wagner's Ring by John L. DiGae-
tani</a></li><li><a href='http://www.pattayadailynews.com/en/2010/09/02/the-bird-scarers-and-
the-scarecrow/' title='The Bird Scarers and the Scarecrow' target='_blank'>The Bird Scar-
```

ers and the Scare-
crow
<a href='http://www.pattayadailynews.com/en/2010/09/01/understanding-
someone%e2%80%99s-decision-to-commit-suicide/' title='Understanding Someone's Decision to Com-
mit Suicide' target='_blank'>Understanding Someone's Deci-
sion to Comm...
<a href='http://www.pattayadailynews.com/en/2010/08/29/laboratory-
made-cornea-gives-hope-for-improved-sight/' title='Lab Corneas Gives Hope for Im-
proved Sight' target='_blank'>Lab Corneas Gives Hope for Im-
proved Sigh...
<a href='http://www.pattayadailynews.com/en/2010/08/29/black-rice-
set-to-be-new-superfood/' title='Black Rice Set to be New Superfood' tar-
get='_blank'>Black Rice Set to be New Super-
food
<a href='http://www.pattayadailynews.com/en/2010/08/26/spirit-houses-
worshipping-the-past-present/' title='Spirit Houses: Traditional Thai Spirit Worship ' tar-
get='_blank'>Spirit Houses: Tradi-
tional Thai Spirit W...
<a href='http://www.pattayadailynews.com/en/2010/08/26/buying-
gold-how-to-know-if-it-is-the-real-thing/' ti-
tle='Buying Gold? How to Know If It Is the Real Thing' tar-
get='_blank'>Buying Gold? How to Know If It Is the Re...
text/disk-part2.img-503424.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-514110.htm:
<a href='http://www.pattayadailynews.com/en/2010/09/05/justice-for-sale-freedom-for-a-
fee/' title='Justice for Sale, Freedom for a Fee' target='_blank'>Justice for Sale, Free-
dom for a Fee
<a href='http://www.pattayadailynews.com/en/2010/09/05/wagner%e2%80%99s-
ring-by-john-l-digaetani/' title='Wagner's Ring by John L. DiGaetani' tar-
get='_blank'>Wagner's Ring by John L. DiGae-
tani
<a href='http://www.pattayadailynews.com/en/2010/09/02/the-bird-scarers-and-
the-scarecrow/' title='The Bird Scarers and the Scarecrow' target='_blank'>The Bird Scar-
ers and the Scare-
crow
<a href='http://www.pattayadailynews.com/en/2010/09/01/understanding-
someone%e2%80%99s-decision-to-commit-suicide/' title='Understanding Someone's Decision to Com-
mit Suicide' target='_blank'>Understanding Someone's Deci-
sion to Comm...
<a href='http://www.pattayadailynews.com/en/2010/08/29/laboratory-
made-cornea-gives-hope-for-improved-sight/' title='Lab Corneas Gives Hope for Im-
proved Sight' target='_blank'>Lab Corneas Gives Hope for Im-
proved Sigh...
<a href='http://www.pattayadailynews.com/en/2010/08/29/black-rice-
set-to-be-new-superfood/' title='Black Rice Set to be New Superfood' tar-
get='_blank'>Black Rice Set to be New Super-
food
<a href='http://www.pattayadailynews.com/en/2010/08/26/spirit-houses-
worshipping-the-past-present/' title='Spirit Houses: Traditional Thai Spirit Worship ' tar-
get='_blank'>Spirit Houses: Tradi-
tional Thai Spirit W...
<a href='http://www.pattayadailynews.com/en/2010/08/26/buying-
gold-how-to-know-if-it-is-the-real-thing/' ti-
tle='Buying Gold? How to Know If It Is the Real Thing' tar-
get='_blank'>Buying Gold? How to Know If It Is the Re...
text/disk-part2.img-589549.js:For example, in john.doe@somewhere.com, john and doe are words.
text/disk-part2.img-589549.js:For example, in john.doe@somewhere.com, john and doe are words.
text/disk-part2.img-683443.js: * Copyright (c) 2008 John Resig (jquery.com)
text/disk-part2.img-724837.js:For example, in john.doe@somewhere.com, john and doe are words.
text/disk-part2.img-724837.js:For example, in john.doe@somewhere.com, john and doe are words.
text/disk-part2.img-732254.htm:
<a href="http://video.msn.com/video.aspx?mkt=en-
au&brand=ninemsn&vid=23c49098-a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_NH_NEWS_TAB_VIDEO','1')"><img src="http://images.ninemsn.com.au/resizer.aspx
tor contestants have punch-up" title="9RAW: Rude X Factor contestants have punch-up" bor-
der="0" align="middle"><a href="http://video.msn.com/video.aspx?mkt=en-
au&brand=ninemsn&vid=23c49098-a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_NH_NEWS_TAB_VIDEO','2')">9RAW: Rude X Factor contes-
tants have punch-upSeptember 05, 2010: Aspir-
ing singers Abbey Johnston and Lisa Parker have shocked X Factor viewers after insult-
ing some of the judge panel and then get-
ting into a fight with each other on stage.
text/disk-part2.img-
732254.htm: <a href="http://video.ninemsn.com.a
a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_MSN+video+category','13')"><img src="http://images.ninemsn.com.au/resizer.as
tor contestants have punch-up" title="9RAW: Rude X Factor contestants have punch-up" bor-
der="0" align="middle"><a href="http://video.ninemsn.com.au/video
a910-49ca-ab72-
cacad38df604" onclick="AdTrack.t(this,'HL_MSN+video+category','14')">9RAW: Rude X Factor con-
testants have punch-upSeptember 05, 2010: Aspir-
ing singers Abbey Johnston and Lisa Parker have shocked X Factor viewers after insult-
ing some of the judge panel and then get-
ting into a fight with each other on stage.
text/disk-part2.img-932806.txt:09/06/2010 01:02:52 <Favorites> folder loca-

```
tion is "C:\Documents and Settings\John S\Favorites".
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ exit
exit
Script done on Sun 17 Oct 2010 18:11:35 EST
Script started on Sun 17 Oct 2010 18:12:49 EST
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ file t
part2.img-932806.txt
text/disk-part2.img-932806.txt: ASCII English text, with CRLF line terminators
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ grep t
part2.img-932806.txt text.txt [C[C[C[C[C[1@-[1@C[1@3[1@
John S/Application Data/Microsoft/Internet Explorer/brndlog.txt
  ASCII English text, with CRLF line terminators
  Image: disk-part2.img  Inode: 932806
  Saved to: text/disk-part2.img-932806.txt
John S/Application Data/Microsoft/Internet Explorer/brndlog.bak
  ASCII text, with CRLF line terminators
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ head t
part2.img-932806.txt
09/06/2010 01:02:52 NoClear flag is specified.
09/06/2010 01:02:52    COM initialized with S_OK success code.
09/06/2010 01:02:52 Branding Internet Explorer...
09/06/2010 01:02:52 Command line is "/mode:isp /peruser".
09/06/2010 01:02:52 Global branding settings are:
09/06/2010 01:02:52    Context is (0x01C00008) "Internet Content Providers, running from per-
user stub";
09/06/2010 01:02:52    Settings file is        "C:\Program Files\Internet Ex-
plorer\Signup\install.ins";
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ tail t
part2.img-932806.txt
09/06/2010 01:02:52    Processing subscriptions...
09/06/2010 01:02:52    There are no subscriptions to process!
09/06/2010 01:02:52    Done.
09/06/2010 01:02:52    Refreshing browser settings...
09/06/2010 01:02:52    Broadcasting "Windows settings change" to all top level windows...
09/06/2010 01:02:52    Done.
09/06/2010 01:02:52 Done.
09/06/2010 01:02:52 Done.
]0;dleigh@alphonse: /var/evidence/sorted_files[01;32mdleigh@alphonse[00m:[01;34m/var/evidence/sorted_files[00m$ exit
exit
Script done on Sun 17 Oct 2010 18:14:50 EST
```

E Transcript Digests

```
1d7b02c90e8b56c8332b93ad62c1f687  browser1
5593ca11b4cc1914dd8b2580b4839994  browser2
5c489c1ce93e9490084cce745ffaffb5  browser3
445e577e6d5a0e2af0acffff153733e3  carve1
2ddf25670faf34a6624216fccd6df30b  cookies
77c0f53a3829817fa70e07dadd7c36d0  delfiles1
90bd2103914d70b230d929e7271b4b5a  delfiles-jason1
a585fbac6e441737feb77f680f825ed9  fat16-carvedfilemd5s
50012e0a0bb003e499d54c36f2d6bd3b  fat16-fsck
497ee12d26e58dea850de97576b4d11c  fat16-initial
8f429ec586aed13fef790f2974338b7b  jason1
c9cc7f11311971e8ef488ce39eb47566  listfiles
f5b147680c16eb68607c0b5889de855a  listfiles2
f2e014291441b0878fb2e68c8efdc0b7  mactime1
35c1fa12c24991042dd5080971b316f8  mactime2
7d52e263b0fab2f92eadc2ab57c9c5da  malware
63c8eb1690067af84fce00bc47e52683  malware2
3433458ea72ac71aa6041d6d2fff79b1  meta-image-1
94557d662b3c0a31b0bedd588c771fef  meta-image-1.5
5187140cfb697a2e8d49fb4fc2d3f580  meta-image-2
13cfa09a0f42301150b78f8a9f08ee9c  mmls-split
6648354cdd72564fc6170417508bac25  nothumbs
66eb006b9d7e33f5cd15387dd7073e35  rardecrypt.txt
ba4a3cd9c1fb2ce47b544b3cf38e348c  registry
fda7a12d5167304b75fe794554106f49  registry2
be2fba3b5db4b86e02fd2d45f65222c2  replica_state_license_plate.gif.txt
0e439e2c8e818448d3ba7fb41e7cdefb  replica_state_license_plate.gif.txt2
d25d6ee2a5db11aee31f95eaf708f4bf  slack1
393c41ab1e1ce5e0f8c39f2053f68d6a  sorter
34fa39cfa32f0c772ee82ce9f2f1304d  sorter2
8e37906fb783b0e9a0a13f5a9149d802  textsearch
c0b6b1f0a4a6661cb4b02e4344425ddf  textsearch2
4cea50c9cd82aff2996f044ffd88c0b9  webcache1
9783c2f59e0ff368bcb726a9720f8e48  webcache2
71d4ba319ca9feaf178a4ae2bf4632ed  webcache3
```