

Cosgrove Computer Systems Inc.

7411 Earldom Avenue
Playa del Rey, California 90293-8058
(310) 823-9448

7/11/2001

**Forensic Examination of Internet Activity
Summary**

The evidence supports the conclusion that the objectionable materials present on Mr. X's computer were obtained during one AOL direct-connect session lasting approximately nine minutes. During this session, ten images were transferred to Mr. X's computer, four of which have been identified by the YZ Police Department as obscene. While Mr. X's Internet activity occasionally included teen pornography sites, none of these visits produced any obscene material, nor did they produce any appreciable volume of artifacts or images. The attributes on the objectionable images indicate that they were transmitted together, during one AOL session, and they probably came from one individual.

Conclusion

The results of the computer examination summarized above indicate that Mr. X acquired the only objectionable material on one occasion during a single period in an AOL download session lasting approximately nine minutes on 2/20/2000 from 2:16AM to 2:25AM. Four of the ten files downloaded were objectionable.

Furthermore, the analysis of Mr. X's Internet activity throughout his possession of the computer showed that his interest in pornographic material was occasional and approximated ten percent total with only one instance of objectionable material as described above (on 2/20/2001).

Examination Process

In compliance with the court's order, on March 12, 2001 we obtained from the YZ Police Department (YZPD) a CD containing a text list of all of the files with their attributes¹ that were found on Mr. X's computer. Several days later, the YZPD created a copy of the defendant's disk for our examination using EnCase² on a hard disk, which we supplied. This image contains an evidentiary record, which is a full clone of Mr. X's disk.

The examination of the EnCase image included inspection of directories involved with the storage of files associated with Internet activity and included the location of the files identified by the YZPD as being objectionable. To that end, an automated procedure provided as a standard examination sequence by the EnCase software, was used to produce an entire record of all Internet activity. In this case, it appears to have included all of the activity since Mr. X purchased the computer on November 15, 1999 (from police records, Officer Y). The report thus produced

¹ File attributes are the characteristics of a file independent of the content. This includes information important to the forensic examiner such as the file's creation date and time, the last time it was modified and the last date of access (last use). Despite the necessity of removing the objectionable files from the subject computer, the critical attribute information was still preserved and is part of the evidence presented.

² EnCase is a commercial software product widely used for computer forensics by law enforcement agencies and computer forensic experts. Preserving the computer evidence with the EnCase image method is the normal procedure used by the YZPD Computer Laboratory. It provides a reliable means of preserving and verifying the integrity of computer evidence. This report is based on the same methods of examination, and using the same software product as the YZPD.

Forensic Examination – Internet Activity Analysis

was examined and the data was converted into a form, which allowed statistics to be compiled and displayed. See Internet Activity.

The AOL Direct-Connect Session

Mr. X claims to have been in an AOL chat room trading pictures with other users. According to Mr. X, users generally share pictures via email. Others advertise that their pictures can be found on other web sites, and they provide links to them. However, one user with the screen name "AbcdUSA006" sent images via AOL download instead. AOL provides more than one mechanism for associating pictures with chat-room communications. In some cases, the pictures are stored in the AOL download directory as occurred in this case. Mr. X, upon opening the message, would have been prompted to download the file containing the picture. Once the file was downloaded to his AOL download directory, it was immediately displayed using AOL's image viewer. In addition, a shortcut to the image was placed in the user's Windows "recent documents" folder. These shortcuts are actually files that share the name of the image but have a filename extension of ".LNK". The evidence supports this theory as all of the images in question reside in the AOL download directory, and there are shortcuts in the Windows "recent documents" folder for all ten images. Our examination showed that the creation time for the link preceded the creation time for the file itself. This gives a means for estimating the times for downloading separate from the delays between each picture.

The computer evidence confirms that the ten files obtained during this session were downloaded very rapidly, one immediately following the one before it. Many of the files were large and required a significant download time for the pictures as shown by the times shown in the attributes listed in the Table below.

Filename	Creation Date
!!!!SHV.jpg	2/20/00 2:16:06AM
!!!!15Jl.jpg < deleted by YZPD >	2/20/00 2:17:04AM
!!!!15F~1.jpg< deleted by YZPD >	2/20/00 2:17:56AM
!!!13VIB.jpg < deleted by YZPD >	2/20/00 2:18:36AM
!!16&17A.jpg	2/20/00 2:19:00AM
Name1.jpg< deleted by YZPD >	2/20/00 2:19:48AM
SOHR5611.jpg	2/20/00 2:21:32AM
Name2~1.jpg	2/20/00 2:22:50AM
!!!!~12.jpg	2/20/00 2:23:26AM
10_Name3-1.art	2/20/00 2:25:24AM

While there are fourteen additional images present in Mr. X's AOL download directory, all of the other images are either non-pornographic, or were clearly legal. The only questionable images seem to occur from this one nine-minute exchange with someone using the name of "AbcdUSA006".

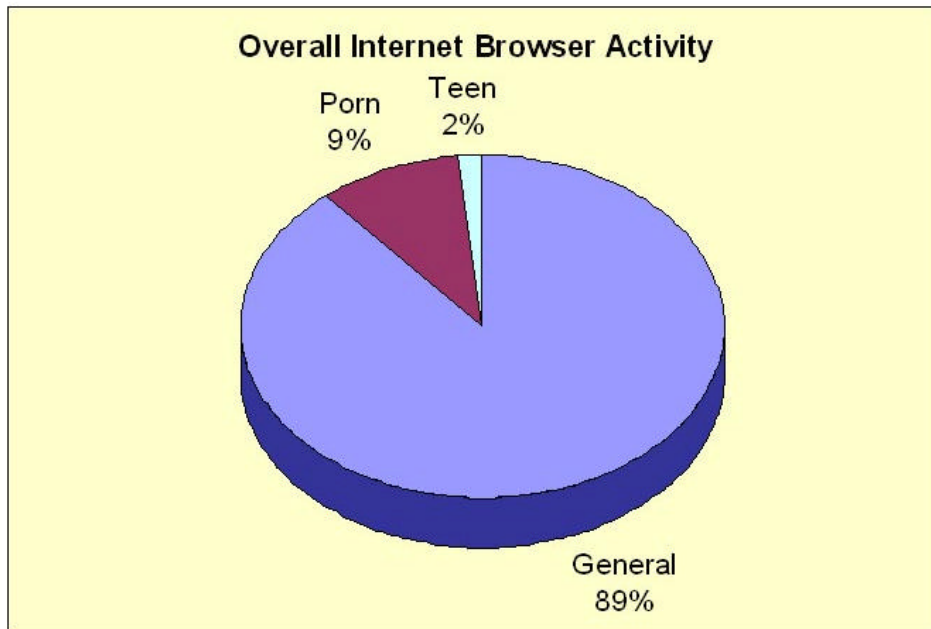
Internet Activity

We analyzed Mr. X's Internet activity during the period 11/23/99 – 2/21/00 to see what kinds of sites he visited. The data indicate that Mr. X was predominately interested in general, non-sexually-related, web sites. Overall, sex sites constituted only eleven percent of Mr. X's Internet visits, and less than two percent of them were obviously questionable.

Type of Site	Number of Visits	Percent Overall Activity
General	4,784	89%
Porn	500	9%
Teen	91	2%

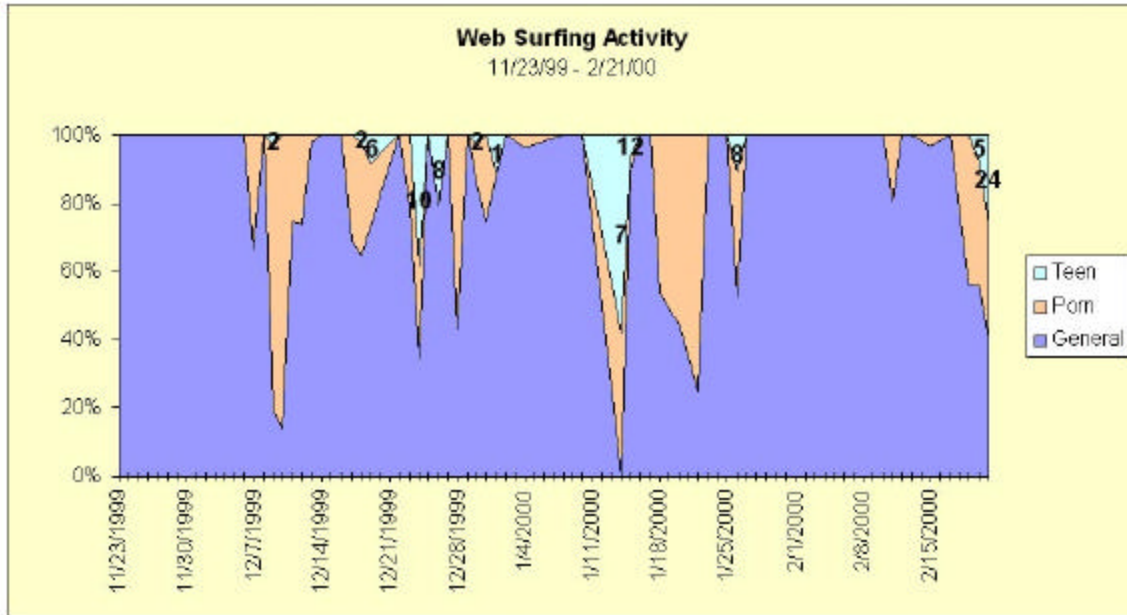
Forensic Examination – Internet Activity Analysis

Total	5,375	100%
-------	-------	------



Additionally, we organized this Internet activity by date to try to determine how regularly Mr. X visited sexually explicit Internet sites. As you can see from the chart below, Mr. X was only occasionally interested in these types of sites, and most importantly, rarely interested in teen sex sites. The numbers printed on the graph represent the number of teen sex sites visited each time they were present in the activity. The data shows that Mr. X only visited teen sex sites on twelve occasions, and because the number of visits are not unique site visits (they could be generated by going back to the same site more than once during a session), the actual number of sites are probably less. In addition, Mr. X claims that many of these teen site visits occurred as a result of clicking on links listed in AOL user's profiles as their personal web site. The fact that users post website addresses in their profiles that redirect browsers to commercial sex sites has been independently confirmed.

Forensic Examination – Internet Activity Analysis



We believe this examination of Mr. X's Internet activity shows that he appeared to be marginally interested in pornography, and the majority of that was not directed towards teenagers. It is likely that some portion of these visits were inadvertent since links indicating something different, often led to these sites. If Mr. X were a habitual collector, we would see many more images present on his hard disk, and much more pornography-related Internet traffic. Furthermore, if Mr. X had probed these teen sites further, he would have left behind dozens of images in his Internet Explorer temporary files folders and in fact the contents of the folders reflect minimal activity.