SWGDE Peer to Peer Technologies

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

1. Purpose

The purpose of this document is to provide guidance in locating potential evidence concerning peer to peer (P2P) file sharing technologies during a forensic examination.

2. Scope

Numerous articles have been written on how P2P networks function, however few have addressed how to forensically examine P2P clients. Therefore, the scope of this research was limited to areas in which trace evidence from some commonly encountered P2P clients (applications) can be found.

3. Introduction

With the increased use of P2P networks for illegal purposes, law enforcement agencies are increasingly being asked to conduct forensic examinations on systems that are utilizing P2P technology. Due to the lack of currently available technical research, SWGDE recognized the need to provide examiners with detailed guidance on areas of possible evidentiary interest on many commonly used P2P client applications. At the request of SWGDE, the Computer Crimes Section of the National White Collar Crime Center (NW3C) conducted detailed research on this topic and provided their findings to SWGDE.

4. Testing Methodology

A. Testing Environment

- a. Windows XP Service Pack 2 and Windows VISTA 32-bit
  - i. VMWare Server 1.0.4
    1. Each client was examined in a separate VMWare machine.
    2. A "bridged" network setting was used, so that each Virtual Machine would have a separate IP Address from the host.
- b. OSX (10.4) and Linux (Sabayon 3.4)
  - i. Each client was examined on a separate stand alone machine.
- c. Base install of the operating systems

B. Client setup

- a. Only the free version of any client was used; usually ad-supported.
- b. Standard Installation Defaults
  - i. To maintain consistency, only the default installation options were accepted

C. The examination of the clients was based on a "checklist" mentality.

a. Default Installation Location

i. Where, by default, does the client install?

ii. Is there a location (such as the registry) that will indicate where a client was installed (whether they chose the default setting or not)?

b. Shared Folders

i. What folder(s) are shared by default?

ii. Where can we find what other folder(s) the user chose to share?

c. Search Term Locations

i. Where can we find what search terms the user had entered?

d. Registry Findings

i. Is there any potentially useful information that was found in the registry that was not covered by another question?

e. Dates and Time Data

i. What date and time information is available within the client, such as log files?

ii. How are MAC times affected by download times?

f. Incomplete Downloads

i. Where, by default, are incomplete (partial) downloads stored?

ii. If possible, how does the client track downloads?

g. Instant Messaging

i. What type of IM does the client use, and does it log the chats?

h. Clients Files Shared To (IP Addresses)

i. Does the client log who has downloaded a file from the client being examined?

i. Uninstall Residue

i. If the user uninstalls a client, what is left over to show that the client was installed at one time?

j. Other Nuggets

i. Client-specific information that could be of evidentiary value, but was not covered in any of the other sections.

ii. Additional, non-evidentiary information that could be of use to the examiner.

5. Results

The results of the research conducted by NW3C have been provided to SWGDE for distribution. These results can be found at SWGDE.org in a report entitled "Peer to Peer: Items of Evidentiary Interest."

6. Limitations

The research was conducted with the P2P clients available for download at the time of testing. Additions and updates to the report may be made periodically as additional research is undertaken.

History: SWGDE Peer to Peer Technologies

Rev #	Issue Date	Section	History
1	02/08/2008		Initial Issue
1	--		Updated document per current SWGDE Policy with new disclaimer. No changes to content and no version/publication date change. (9/27/2014)

Errata Sheet

Name of Document and Version#

Page #	Section	Comments