Limewire Examinations

By

Joseph Lewthwaite, Victoria Smith

Presented At

The Digital Forensic Research Conference

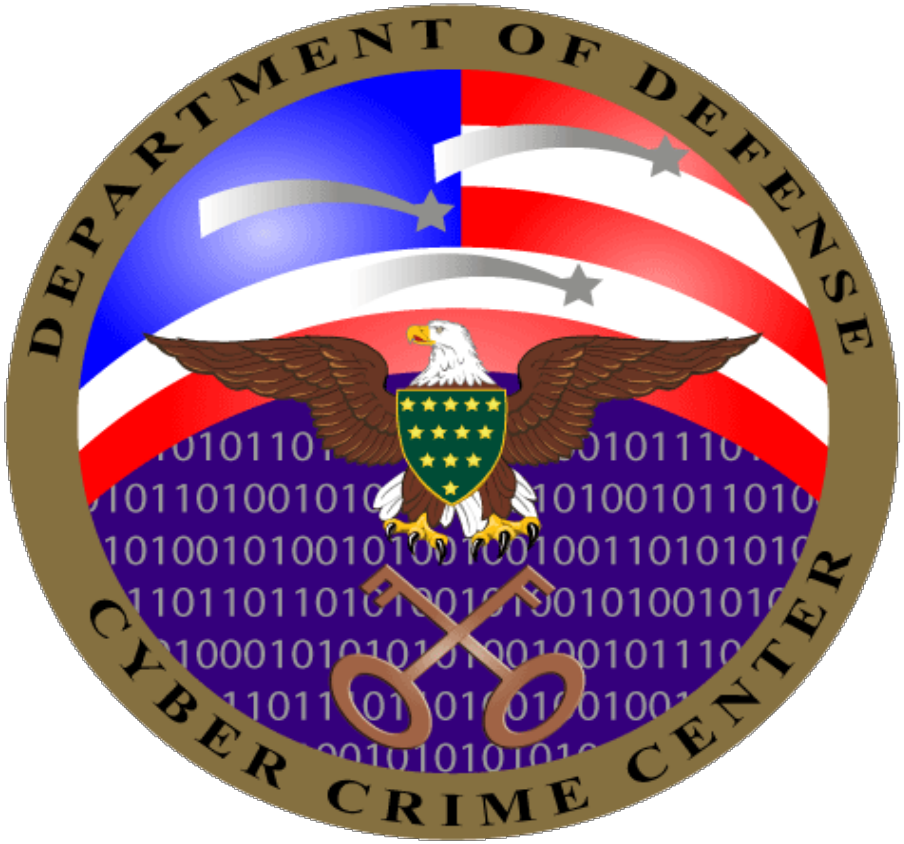
DFRWS 2008 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Limewire Examinations

DC3



DFRWS 2008

12 August, 2008

Introduction

DC3

- **Joseph Lewthwaite**
  - Researcher, software engineer with the Defense Cyber Crime Institute.
  - Contractor General Dynamics AIS
- **Victoria Smith**
  - Forensic Examiner, Litigation Support Section in the Defense Computer Forensic Laboratory
  - Contractor General Dynamics AIS

Overview

DC3

- Introduction to Limewire
- Downloads and Sharing
- Files and the evidence they contain
- Showing Intent - Search Terms
- Artifact Scan – Tool to parse the evidence.

Limewire

DC3

- Limewire is one of the more popular Gnutella P2P clients
- It features in many of the Labs cases
- Open Source though it is backed by a company
- Java application
- Serialization adheres to the Java Object Serialization spec.
- This all means the binary data can be read, yields dates and times, ratings, IP addresses…

Share / Download Model

DC3

- Limewires' sharing download model has evolved over the years.
- Initial Model:
  - Download to the shared directory
  - Could share anything
  - 'Library.dat' solely contained exceptions to the sharing made by the user.
- New Model
  - Downloads and Share directories have been separated
  - For security concerns the root of a drive cannot be shared
  - 'Library.dat' now contains entries made by Limewire as it shares downloads individually.

Evidence of Sharing

DC3

- **Limewire.props – Runtime properties**
  - DIRECTORY_FOR_SAVING_FILES
  - DIRECTORIES_TO_SEARCH_FOR_FILES
  - MAX_HARD_UPLOADS – Upload connections
- **Fileurns.cache – Listing of files, name and SHA1, and when they were added to the users library**
  - **Does not tell you whether they were downloaded or copied/moved**
- **Library.dat – User exceptions to the general directory shares.**
  - **File entries made by Limewire will tell you what was downloaded, the file path matches the save directory.**

Abuser Flag

DC3

- Fileurns.cache – Contains file name, SHA1 value and time the file hit the users' library
- Createtimes.cache – Contains SHA1 values and the time the file hit the network
- Matching times or times that are close would be an indicator the suspect is adding new files.

Penetrating the Networks

DC3

- Limewire does not log IP addresses and what came from where but there are two sources that can be used to expand the investigation
- Gnutella.net – Listing of ultrapeer nodes, IP addresses, the client can use to connect to the Gnutella network.
- Spam.dat – Listing of peers, IP addresses, the client has had contact with.
  - Spam filter rates each IP as to its relevance.
  - Age, score
  - Keywords

User Searches and Intent

DC3

- Computers that connect to the Gnutella network using the Limewire client do so in one of two roles, as a leaf or ultrapeer
- Ultrapeers handle all network traffic and a full participants in the network
- Leaves connect to other leaves only to download files
- HTTP used to connect leaves for downloading files

User Searches

DC3

- Default setting length of 30 characters for search term
- Search query is routed to ultrapeer that conducts the query search on behalf of the leaf and returns the results to the requesting leaf
- Results include the name, IP address and SHA1 value (base 32) of the file

Search Terms

DC3

- Limewire does not retain the user input search terms in any logical file on the system
- However, Limewire does retain the search term for the last file download that was not completed
- This search term can be located in the downloads.dat file in the Incomplete folder

Search Terms and Downloading Files

DC3

- Limewire starts the downloading of a file by placing that file in the Incomplete folder
- Limewire creates an entry in the downloads.dat for the file retaining the IP address of source, SHA1 value and the search term used to locate the file
- The file is given a temporary name consisting of ‘T - %size of file% and name of file including extension

Search Terms and Downloading Files

DC3

- Once the download has completed the entry for the file is moved to the designated shared folder
- The downloads.dat file is refreshed and the data deleted
- This allows for possible recovery from unallocated clusters of deleted downloads.dat file that contain the search terms

Search Terms and Downloading Files

DC3

- Testing has shown that user initiated cancellation of a download does not have the search term retained in the downloads.dat file, but the entry for the file remains in the file

- Removing files by manually deleting them from the Incomplete folder will refresh the downloads.dat file to no longer retain the entry for the file.

Locating User Search Terms

DC3

- **Locating the deleted downloads.dat files and data related to the user search in unallocated clusters can be accomplished by using the following search keywords:**

  searchinformationmaps

  title=

  queryt

Locating User Search Terms

DC3

- **The following data from unallocated clusters illustrates the location of the user search term from a recovered deleted downloads.dat file:**

attributessq·~·.?@··w···t··searchInformationMapsq·~·.?@···w··t··mediasr·
com.limegroup.gnutella.MediaType7□ †ia;]•···Z· isDefaultL··descriptionKeyq·~· L··extsq·~·
L··schemaq·~·xp·t··Videosr··java.util.TreeSetÝ˜P“•í‡
··xpsr·Corg.Limewire.collection.Comparators$CaseInsensitiveStringComparator·¦Í~s¬BÌ···x
pw····1t··asft··asxt··avit··cdgt··dcrt··divt··divxt··dvt··dvdt··dvxt··flct··flit··flvt··flxt··idxt··jvet··m1v
t··m2pt··m2vt··mkvt··mngt··movt··mp2t··mp2vt··mp4t··mpet··mpegt··mpgt··mpgvt··mpvt··mpv
2t··nsvt··ogmt··qtt··ramt··rmt··rmmt··rmvbt··rvt··smit··smilt··srtt··subt··swft··vcdt··vobt··vrmlt··
wmlt··wmvxt··videot··queryt·casablancat··xmlt·‹<?xml
version="1.0"?><videosxsi:noNamespaceSchemaLocation="http://www.Limewire.com/sch
emas/video.xsd"><video title="casablanca"/></videos>t··typesr··java.lang.Integer·â ¤÷•□
‡8···l··valuexr··java.lang.Number†¬•··”à‹···xp····t··titlet· casablancaxxt··sha1Urnq·~·
¬t··defaultFileNameq·~·dt··fileSizesr··java.lang.Long;‹ä□Ì□#ß···J··valuexq·~·õ····+‰ÄÒt··save
Filesq·~·wt·RC:\Documents and Settings\LaCFG\My Documents\Limewire\Saved\
Casablanca (b & w).aviw··\xxxxq·~·u

Word of Caution

DC3

- Testing of Limewire has resulted in the location of data in the pagefile.sys of Windows OSs data of searches that are not associated with user activity but are indicative of ultrapeer activity.

Word of Caution

DC3

- **Data recovered from a Windows XP pagefile.sys file:**

h=À·ÈÍÀ·····ÿÿÿÿ·····ËÀ·äõ:Bÿ···?xml version="1.0"?><audios xsi:noNamespaceSchemaLocation="http://www.limewire.com/schemas/audio.xsd"><audio title="snowpatrol"/></audios>· Ã·MA·,SO@·|„)à&· Œ³¡®5T·Đ····@····ÙxÌ"S····· ·Ã·DHTC····DUB‹··GUEA··LOCCnl··TLS@·UPC·$·,VCELIME·(D· Ûs· ĐwZ R¤ž»Þ· ƒLOCBen·ò8iÝu›½·7·5·· tp····A···Ê·YdeÃB·····Ã·DHTC····DUC€Q··GUEA··LOCCen· ·TLS@·UPC···,VCELIME·ûŠÏAdÆ`v· ½\ˆÂ÷H····@···ËbD!þ2·····Ã·DHTC····DUBy4· GUEA··LOCCen··TLS@·UPC···,VCELIME··c§Ò«·òœ·ÚÍxŠ¿·····@···ù)ONJÿ®·····Ã· DHTC····DUBG··GUEA··LOCCen··TLS@·UPC···,VCELIME·G½9·I·”ÚŸÏ„□ ’³<€··¡···€· kinky jpg·<?xml version="1.0"?><images xsi:noNamespaceSchemaLocation="http://www.limewire.com/schemas/image.xsd"><image title="kinky jpg"/></images>·Ã·MA ,SO@·7ü· ©òf·ìÿ°ñ§3û··€· à·DSC00265.JPG·C¾†□ <½:‹ÎÁr8rH-€··©···€·metallica vs·<?xml version="1.0"?><audios xsi:noNamespaceSchemaLocation="http://www.limewire.com/schemas/audio.xsd"><audio artist="metallica vs."/></audios>·Ã·MA·, SO@·žÈ”èýQI·ruÓ¥ŸíÌ···@···Ë”·ò3Kê···Ã·DHTC

AScan

DC3

- Java Command line tool
- Parses a variety of P2P artifacts:
  - Limewire
  - Bearshare
  - Ares
- Outputs as HTML, comma delimited and XML
- Available from the NRDFI (www.nrdfi.net) to eligible law enforcement personnel, email join@nrdfi.net.

Future

DC3

- AScan
  - Different clients as needed
  - Keeping up with changes in versions
  - Developing software and techniques in mapping out the networks of traders.

Questions?

DC3

- **Contact Info:**
  - joseph.lewthwaite.ctr@dc3.mil
  - victoria.smith.ctr@dc3.mil

Department of Defense Cyber Crime Center

DC3

DC3