L0phtCrack Password Auditor v7

Table of contents

Introduction

Documentation

Getting Started

Security experts from industry, government, and academia agree that weak passwords represent one of the ten most critical Internet security threats, and are receiving more attention as a source of vulnerability, both on client desktop computers and in networks. L0phtCrack 7 identifies and assesses password vulnerability

over local and remote machines in a streamlined application, with built-in reports and remediation tools.

L0phtCrack 7 uses a variety of sources and methods to retrieve passwords from the operating system. Feedback about the strength of passwords is based upon the types of audit required to recover the password, and the length of time required for the audit. L0phtCrack 7 is a state of the art tool for password auditing and recovery that serves to guide organizational policies and procedures.

System administrators audit passwords to determine the strength of the passwords used on client machines and for network access. Weak passwords, such as a password based on a dictionary word, represent vulnerability points for any organization. Administrators use corporate password policies and filtered password generators to improve the quality of passwords used in their organizations. But without testing the passwords against a real world password auditor, the administrator risks the chance passwords can be uncovered by an external attacker or malicious insider. Freely available password cracking programs take into account the ways users select passwords in light of corporate password policies such as requiring the use of numbers and symbols. Many don't realize Patri0ts! as a password is just as easy to guess as patriots was in the past.

L0phtCrack 7 can be used to streamline the migration or upgrading of users from one authentication system to another by computing all user passwords. L0phtCrack 7 is also an excellent auditing tool that Administrators can use to detect weak passwords.

L0phtCrack 7 is available in the following versions:

FEATURE	PROFESSIONAL	ADMINISTRATOR	ENTERPRISE
Password assessment	X	X	X
Password recovery	X	X	X
Dictionary support	X	X	X
Hybrid support	X	X	X
Brute force support	X	X	X
International character support	X	X	X
Wizard-based GUI	X	X	X
Remediation	X	X	X
Windows support	X	X	X
UNIX support	X	X	X
Remote system scans	X	X	X
GPU Support	X	X	X
Assessment scheduling		X	X
Perpetual use	X	X	X
Accounts	500	5000	Unlimited

Next:

[Installing L0phtCrack 7]
How to install L0phtCrack 7 on your computer

[Running L0phtCrack 7 for the First Time]
What to expect the first time

Uninstalling L0phtCrack 7
How to remove L0phtCrack 7 from your computer

Activating L0phtCrack 7
How to activate a purchased copy of L0phtCrack 7 with your license code.

Reinstalling L0phtCrack 7
How to reinstall and reactivate L0phtCrack 7 if you have uninstalled it.

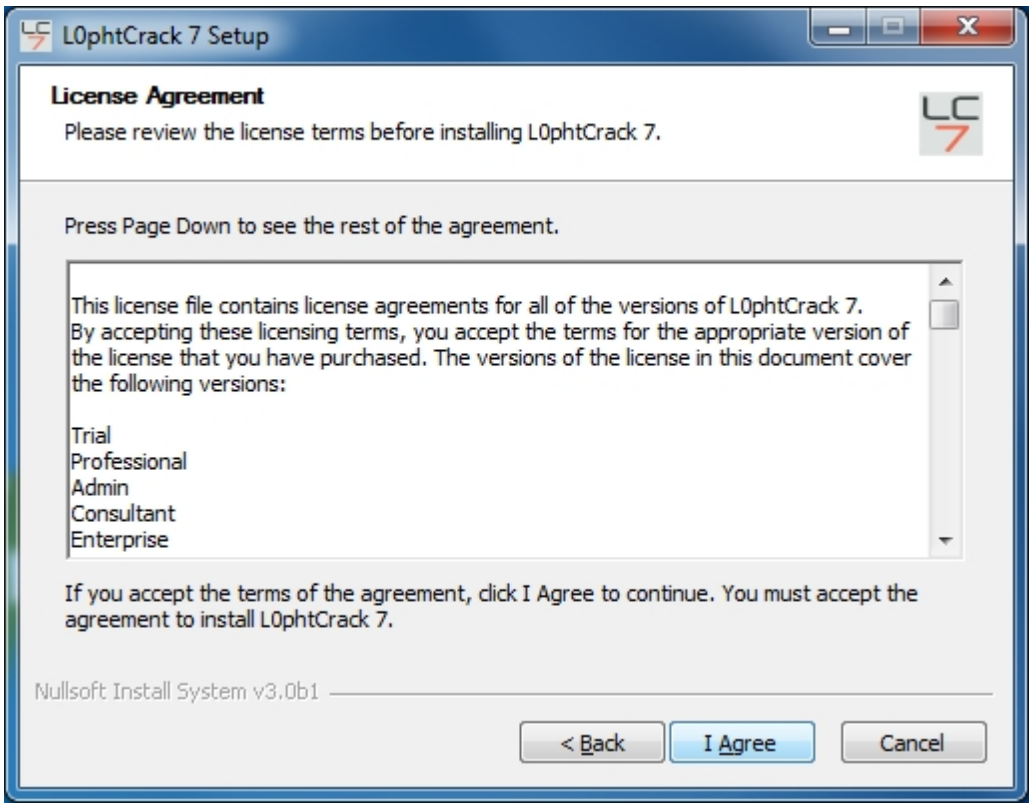
Remote Manual Installation of LC Agent
How to use the remote password dumping agent manually if your organizational needs require it.

Installing L0phtCrack 7

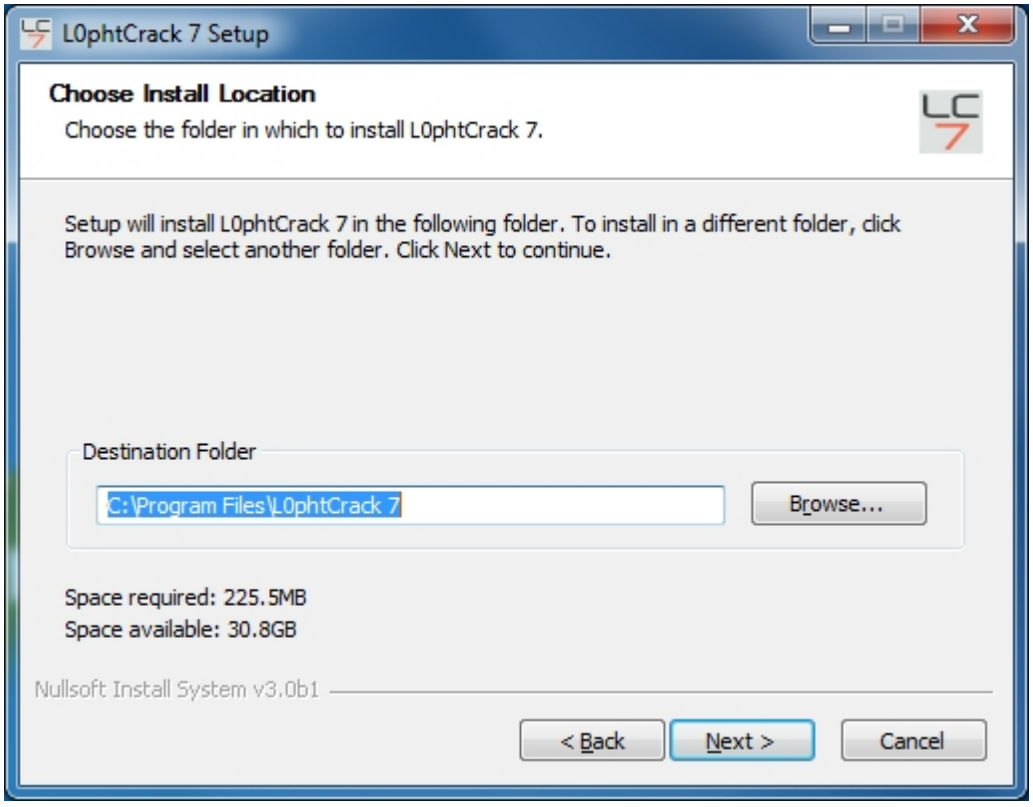
To install L0phtCrack 7:

1. L0phtCrack 7 is distributed in a self-installing executable distribution file that can be downloaded for free at http://www.l0phtcrack.com/download.html.
2. Save the .exe file to your download directory.
3. In the download directory, double click the lc7setup.exe file. The installer starts a standard installation process. At the Welcome screen, click Next.

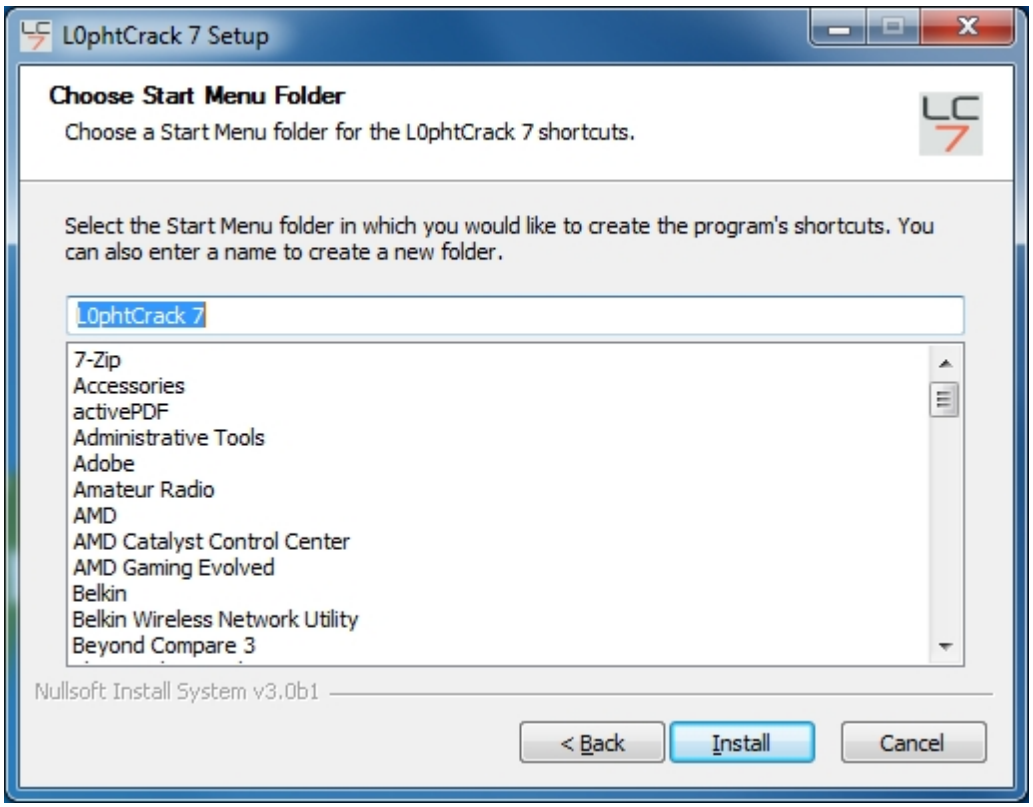
4. Read the License Agreement screen, then click I Agree to agree.



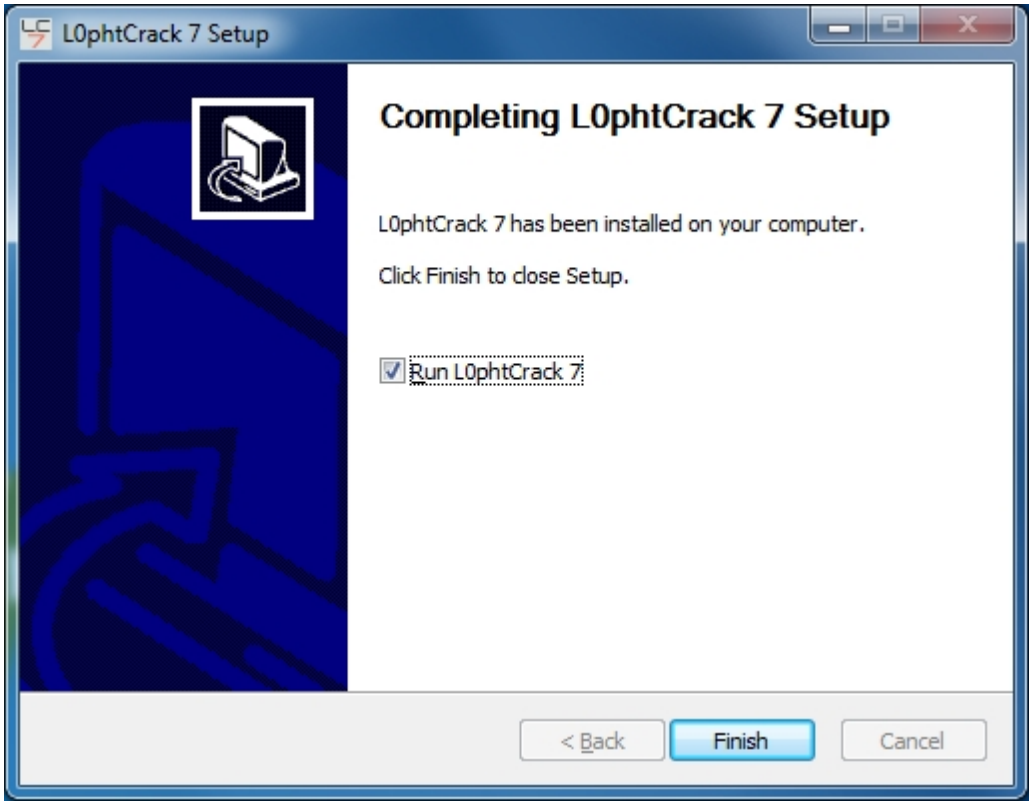
5. The installer installs L0phtCrack 7 in a default installation location: "C:\Program Files\L0phtCrack 7" or you may Browse to choose a different location. Click Next when ready.



6. A shortcut to the L0phtCrack 7 executable is installed in the Programs folder under the Start menu. The default folder name is L0phtCrack 7. You may choose a different name. Click Install when ready.



7. Click Finish when the L0phtCrack installer completes the installation. L0phtCrack will launch by default. If you don't want to run the program at this time, uncheck Run L0phtCrack 7.

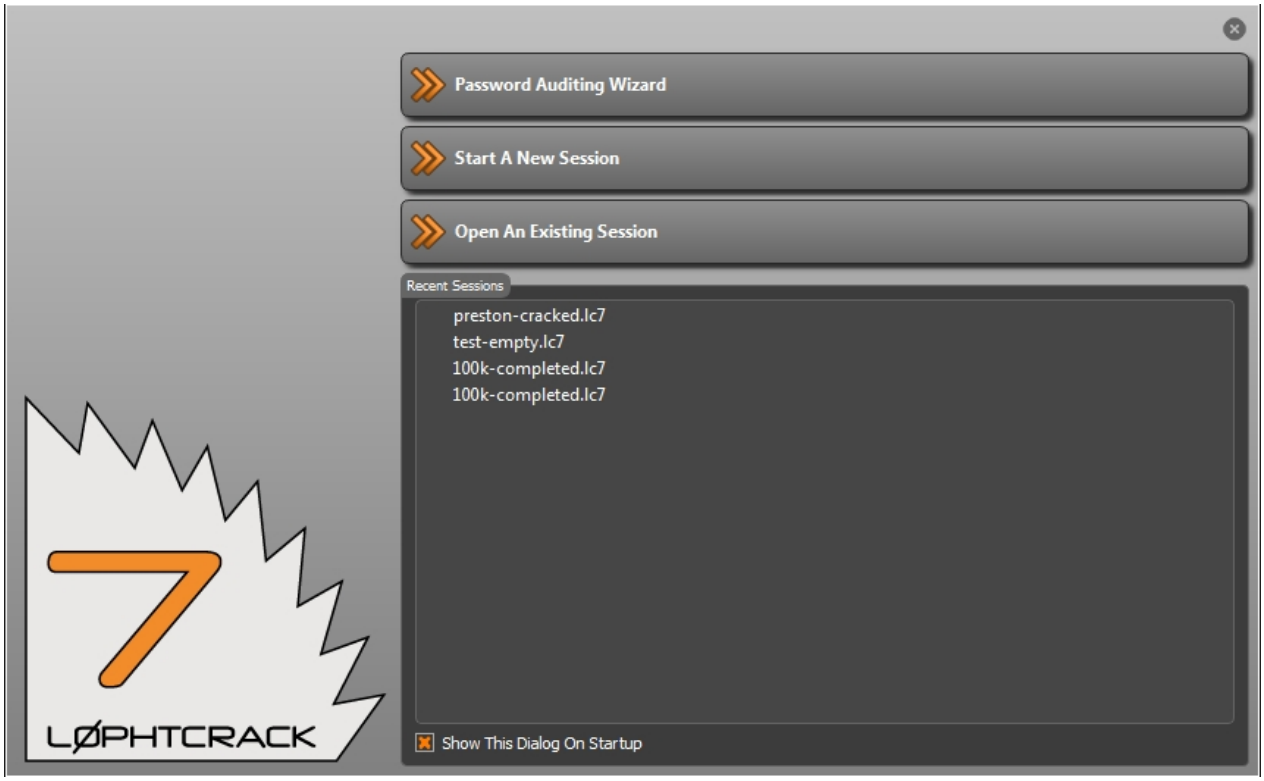


8. L0phtCrack 7 is now installed on your system. You may now click the Start button, and go to the Programs folder to run L0phtCrack 7.

Running L0phtCrack 7 for the First Time

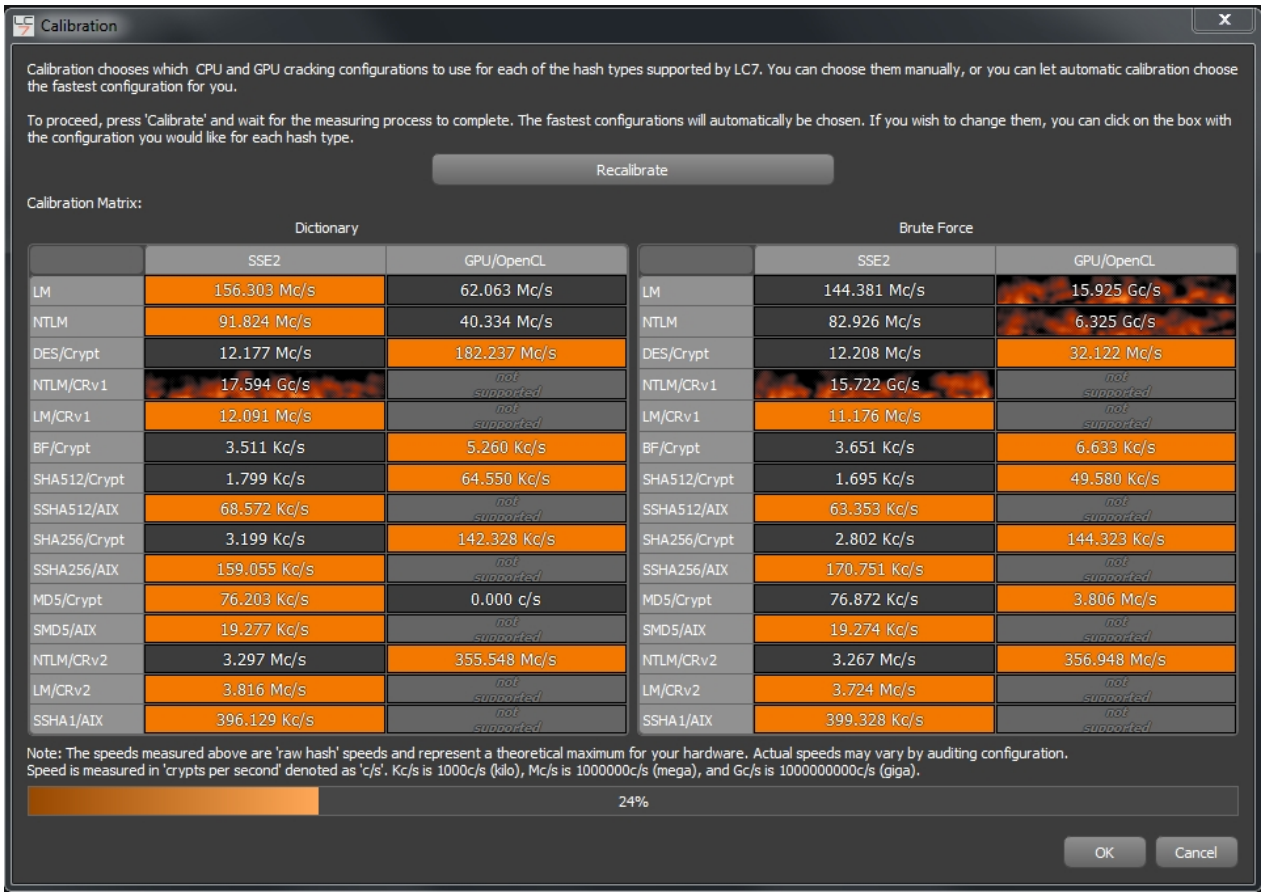
Running L0phtCrack the first time

When L0phtCrack runs for the first time you will see the **Startup Dialog**. From here you can run the **Password Auditing Wizard**, **Start a New Session**, **Open An Existing Session**, or select one of the **Recent Sessions** displayed. You can deselect **Show This Dialog On Startup** to stop displaying the **Startup Dialog** when L0phtCrack starts.



When you run an audit session the first time you will be prompted to optionally **Perform Calibration.** L0phtCrack can select between different processors and processor instructions available to optimize the speed of the password auditting process. L0phtcrack can run a calibration to detect the performance of the available options. This is highly recommended.

Calibration takes several minutes as L0phtCrack tries all the available cracking algorithms across the available CPU instructions and a GPU if present. You can display the Calibration results at any time from the MENU by selecting **Perform Calibration**. You can recalibrate by selecting **Recalibrate**. You will want to do this if you have updated your CPU or GPU hardware.

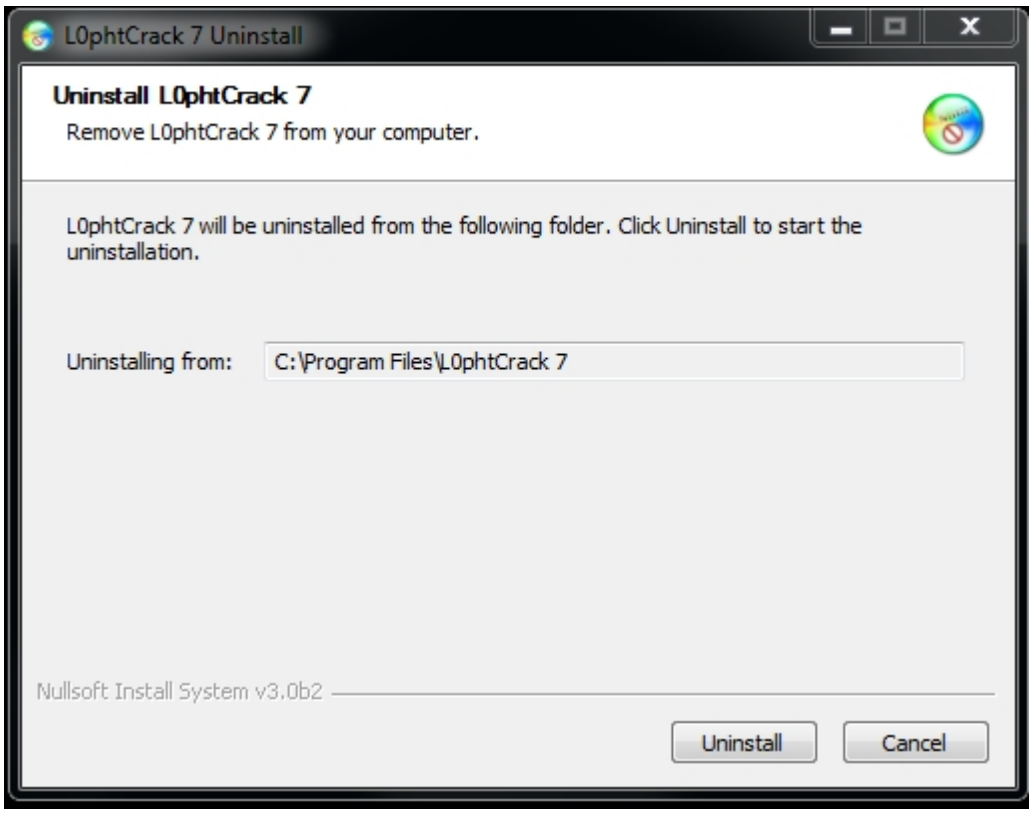


The row header is the hash type. The column header is the CPU instruction set or GPU algorithm used. The speed is listed in Kc/s (Kilocracks/s), Mc/s (Megacracks/s) or Gc/s (Gigacracks/s). L0phtCrack will highlight the fastest algorith in orange or flames if the speed is over 1 Gc/s. The highlighted algorithm will be stored and used in subsequent audit sessions.

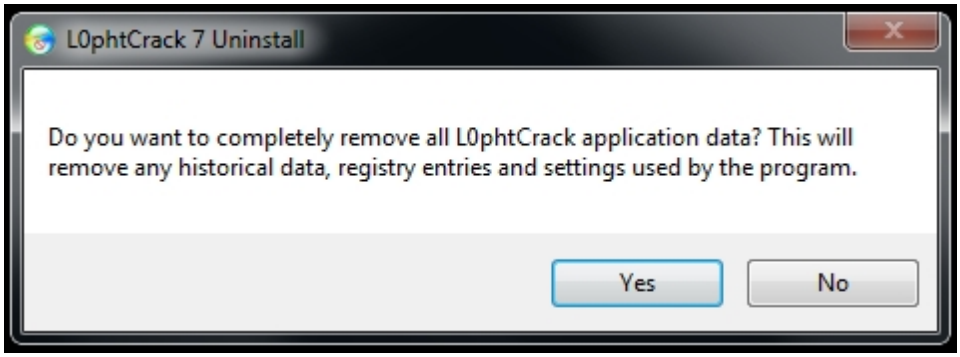
Uninstalling L0phtCrack 7

To uninstall L0phtCrack 7:

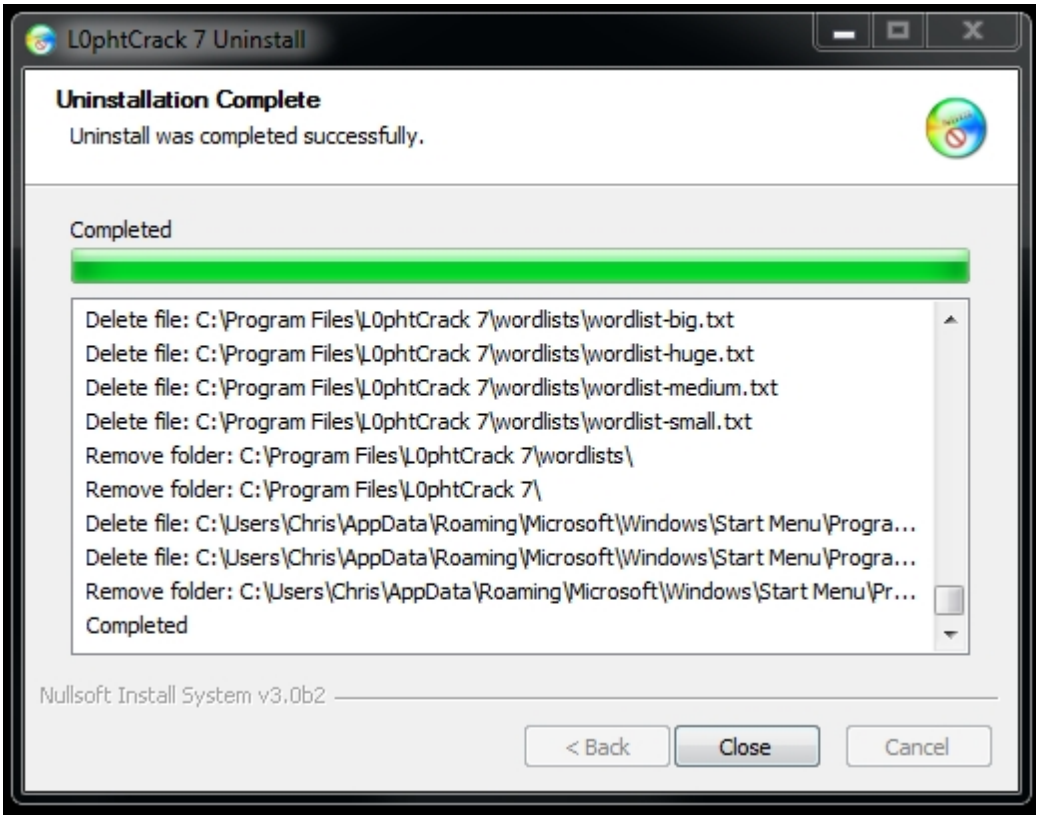
1. In the Windows Control Panel, open Programs and Features.
2. Select L0phtCrack 7 from the list of programs installed on your system.
3. An installer window informs you of your choice to uninstall L0phtCrack 7.



4. Confirm that you want to delete the files by clicking Uninstall.
5. The uninstaller will bring up a prompt asking if you want to remove application data. If you want to remove the data, select Yes. If not, select no.



6. The uninstaller will now remove the L0phtCrack 7 files from your system.



7. L0phtCrack 7 is now uninstalled from your system. Select Close.

Activating L0phtCrack 7

L0phtCrack offers a 15 day free trial period for L0phtCrack 7, providing access to the all features for 5 user accounts.

The following are unavailable in the trial version:

Select **Proceed with Trial** to use the free 15 day trial.

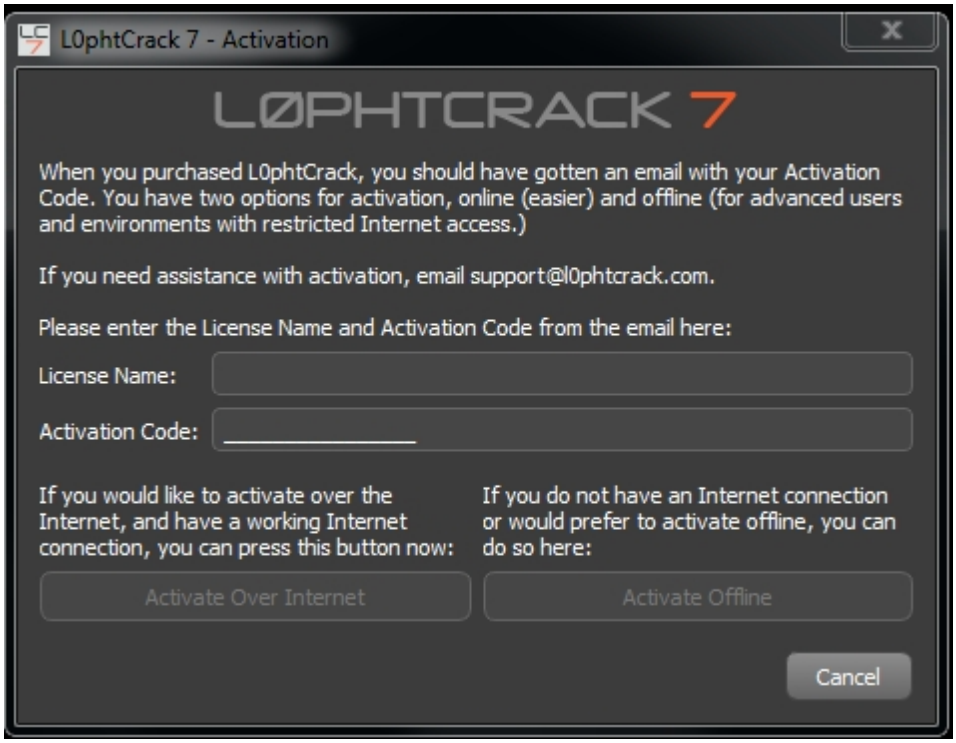
You need to purchase a license and activate L0phtCrack 7 to continue using it after 15 days.

Select **Purchase License** to be directed to our online store to purchase a license to one of the 3 different L0phtCrack 7 editions: Professional, Administrator, or Enterprise. Feature differences between the different editions are listed in a table near the top of this page.

Select **Activate License** once you have obtained you license key. It should have arrived in the email confirming your purchase of L0phtcrack 7.

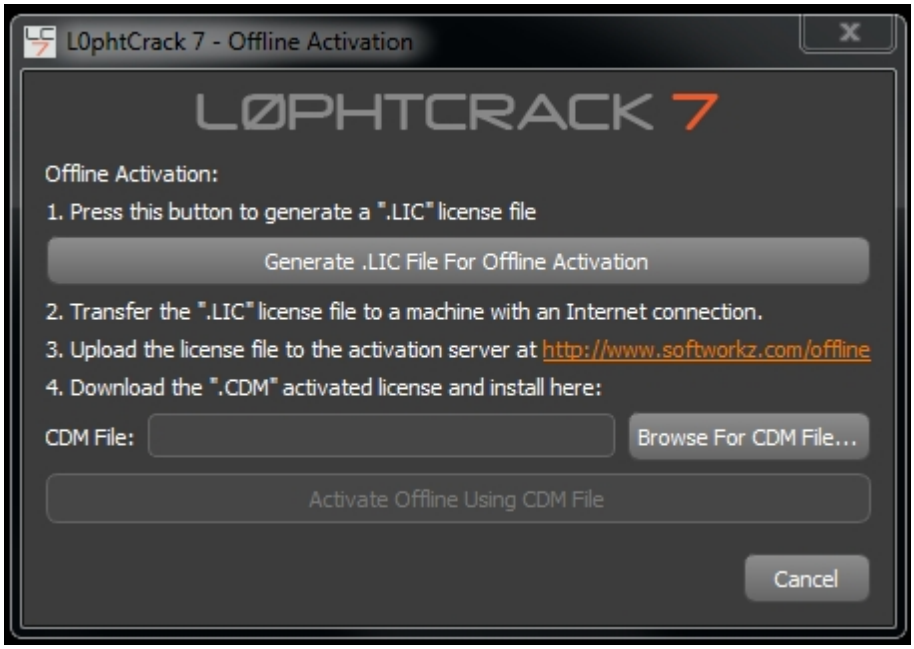
L0phtCrack offers licenses for purchase online, by email or by telephone. Click here for email, phone numbers, and the online purchasing.

L0phtCrack 7 is licensed on a per machine basis, and each machine must be activated with a license. When activating, provide your name, and the Licence Key. It will be 15 alphanumeric digits and look like this: 5SUYF3V4BN82JJFF



You can Activate Over Internet if you have an internet connection from the machine you are activating. If you have no internet connection you can Activate Offline.

When activating over the internet you must enter a password. This allows you to manage the license later online at: http://www.softworkz.com/mylicense. You will need this password if you choose to move your license to a new machine. It is highly recommended that you enter an email address so you can reset the password associated with the license. After you have entered the passwords and an email address select Activate Online.



You can activate offline by generating a .LIC file, moving it to an internet connected machine and uploading to the license server at: http://www.softworkz.com/offline. This will generate a .CDM fle that you will download and move to the machine you want to activate. Once the .CDM is on the machine you want to activate, browse to it and then select Activate Offline Using CDM file.

Reinstalling L0phtCrack 7

To install L0phtCrack 7 on a new machine or operating system, you will need to activate the new installation using your original license key and the password you assigned to it.

To move your license to a new machine you must first deactivate the license on the machine is is currently installed on. You do this by going to the **Settings** page by selecting **Settings** on the left panel. On the **Settings** page select the **About L0phtCrack 7** tab. Next click on the **Deactivate License** button. You will be prompted to enter in your license password. If you have forgotten it you can select I forgot my password to have a password reminder sent to the email address you registered your license with.

Once you have deactivated your license you can then install L0phtCrack 7 on a new machine (download link: http://lc7.download/win64) and then activate the license on the new machine.

Enter the old password for the license and set a new password. If you forgot your old password you can have it reset at http://www.softworkz.com/mylicense. The select Reactivate Online.

What's New in L0phtCrack 7

L0phtCrack 7 includes enhancements and additions to the critically-acclaimed L0phtCrack auditor:

- **All New Cracking Engine:**
  L0phtCrack 7's cracking engine has been completely replaced with a state-of-the-art cracking engine, John the Ripper. Performance is greatly improved for dictionary and brute force audits. Many more password hash types are now supported.

- **GPU Support:**
  Harnessing the computing capabilities of GPUs in graphics cards is a significant advance in password auditing. GPUs can be faster than traditional CPUs for certain password auditing operations. L0phtCrack 7 now supports the two most popular GPUs: AMD Radeon and NVIDIA. Password audits now take hours instead of days. L0phtCrack can support multiple GPU cards for exceptionally fast password auditing. A new calibration process selects the fastest cracking algorithm for the machine's CPU and GPU.

- **Improved Unix Password Support:**

L0phtCrack 7 imports and cracks Unix password files from Linux, Solaris, OpenBSD, FreeBSD, and AIX systems. Password hashes can be imported remotely via SSH or from shadow files or passwd plus shadow files for more user detail. Perform password audits of Windows and Unix from a single interface.

- **Remote Windows Password Import Improvements:**
  L0phtCrack 7's remote Windows password import agent can now work over SMB so you don't have to open any additional ports or make configuration changes to the way you already remotely manage a machine.

- **Audit Scheduler Interface Improvements:**
  System administrators can schedule routine audits as before. Audits can be performed daily, weekly, monthly, or just once, depending on the organization's auditing requirements. The scheduling interface is much improved. Visibility into multiple jobs is possible.

- **Plug-in Support:**
  L0phtCrack 7 is now extensible through a plug-in interface. New password hash importers, new password hash cracking support, and new reporting functionality can be added by 3rd parties and easily installed by end users.

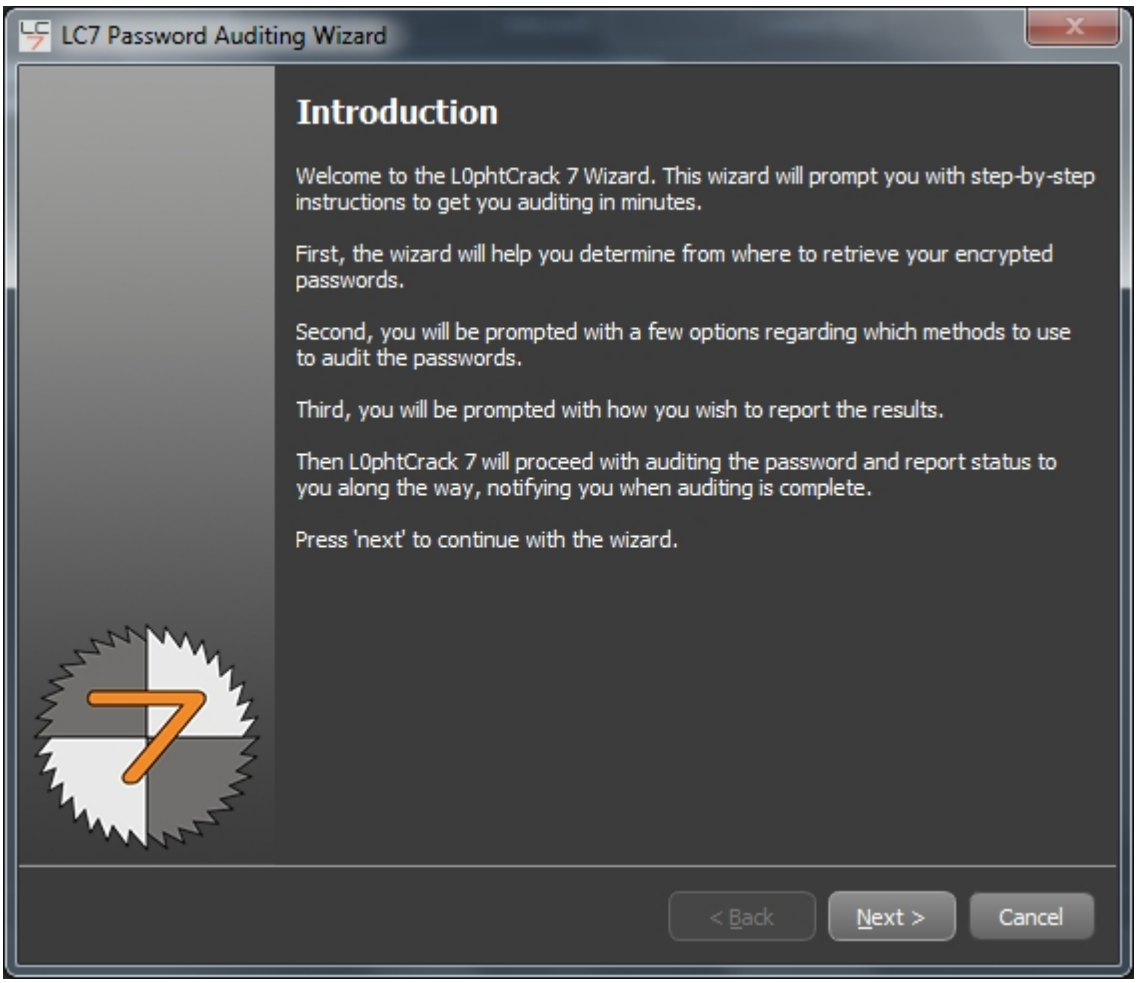
- **Updated GUI:**
  The user interface is improved and updated. A new improved wizard makes common auditing tasks easy for first time users. Advanced users have precise control over importing from multiple systems and fine tuning their auditing job. Current status while an audit is running is clear and responsive.

Quick Start with the L0phtCrack 7 Wizard

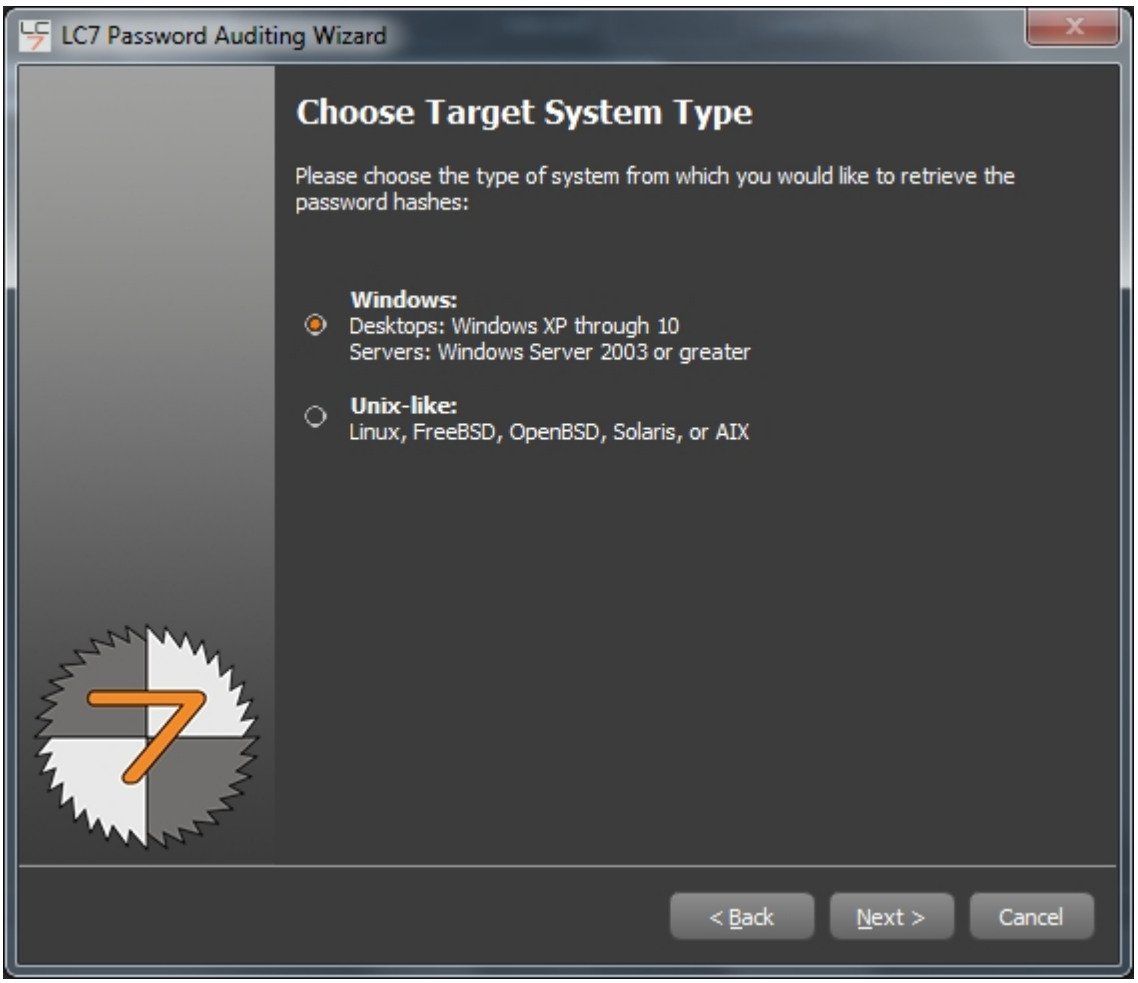
Wizard Overview

The L0phtCrack 7 Wizard helps you quickly configure the settings needed to retrieve and audit passwords by the most common means and provides a quick overview of the password auditing process.

When L0phtCrack first starts, the startup dialog gives you the option of selecting **Password Auditing Wizard**, **Start A New Session**, or **Open An Existing Session**, with a quick selection of recent sessions. The startup dialog opens by default the first time you run L0phtCrack 7. To use L0phtCrack without the startup dialog, uncheck the **Show This Dialog On Startup** checkbox. The Wizard can be launched at a later time from the L0phtCrack 7 menu.
If you select **Password Auditing Wizard** you will start the wizard and see the **Introduction** dialog. Select **Next** to continue.



Choose The System Type To Audit



The Wizard's **Choose Target System Type** dialog selects the type of system you want to audit. There are two options options. Select **Windows** or **Unix-like** then press **Next**.

Select Windows Import Type

If you chose a **Windows** system type the next dialog selects the source of encrypted Windows passwords to audit. There are four options.

- Local machine - L0phtCrack 7 retrieves passwords on the machine it is installed on. This option requires local administrative privileges.
- Remote machine via SMB - L0phtCrack 7 retrieves passwords from a remote machine on the network, provided you have admin privileges on the remote machine. Remote Active Directory machines will require domain admin privileges. SMB filesharing must be enabled on the remote machine.
- File Generated by PWDump, FGDump or compatible tool - L0phtCrack 7 can import password hash files created by external utilities that are compatible with the PWDump format.

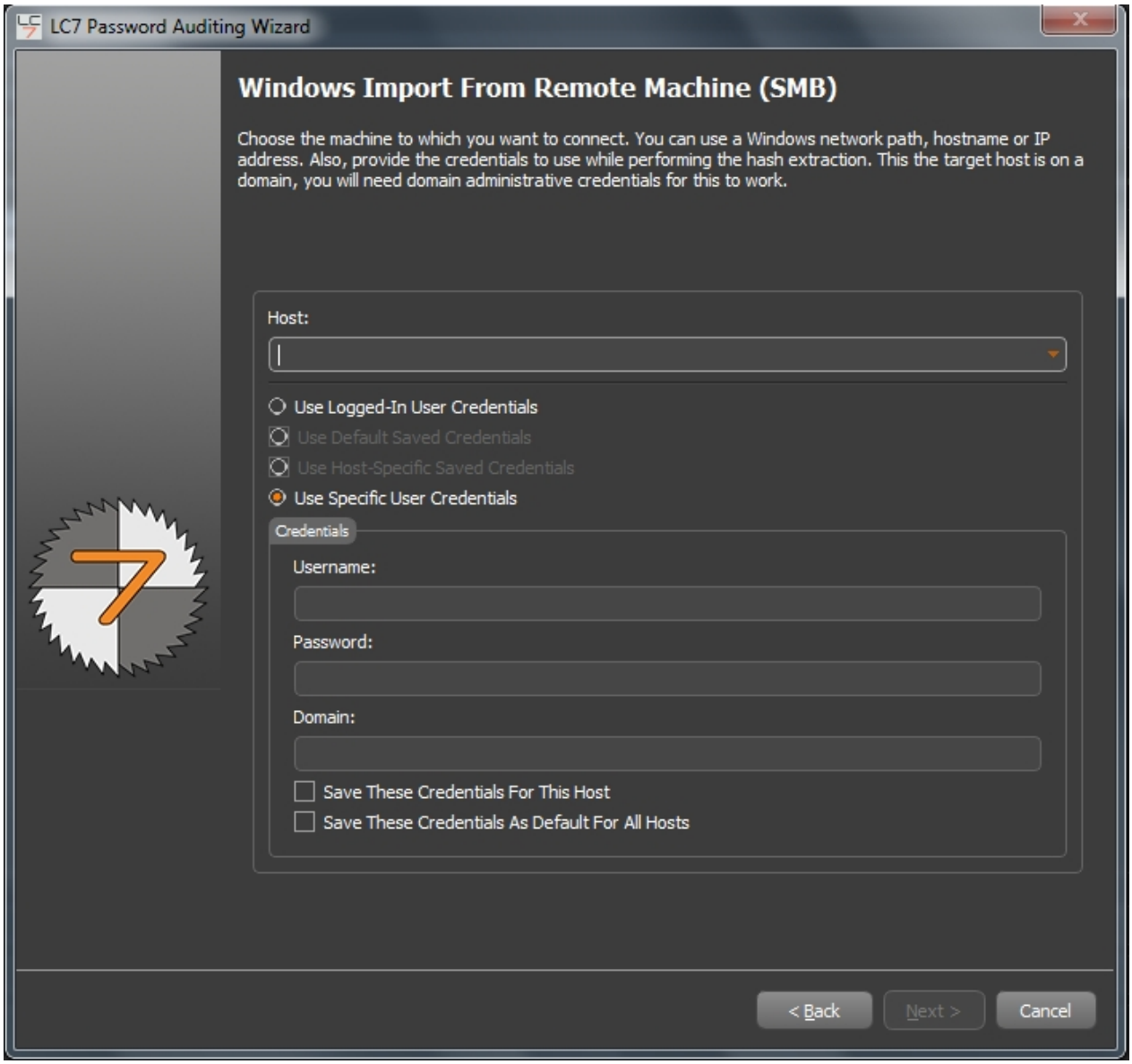
Windows Local Machine

To retrieve password hashes from the local machine you need local admin privileges.

If you are logged in with admin privileges you can select **Use Logged-In User Credentials**.
If you previously saved credentials for the local machine you can select **Use Saved Credentials**.
If you are not logged in to the local machine with admin privileges you can enter admin credentials by selecting **Use Specific User Credentials** and entering Username, Password, and Domain.
If you are entering in credentials you have the option to select **Save These Credentials** to save them in the Windows Protected Store for later usage with the **Use Saved Credentials** option.

Press **Next** to continue on to select audit type

Windows Remote Machine Via SMB



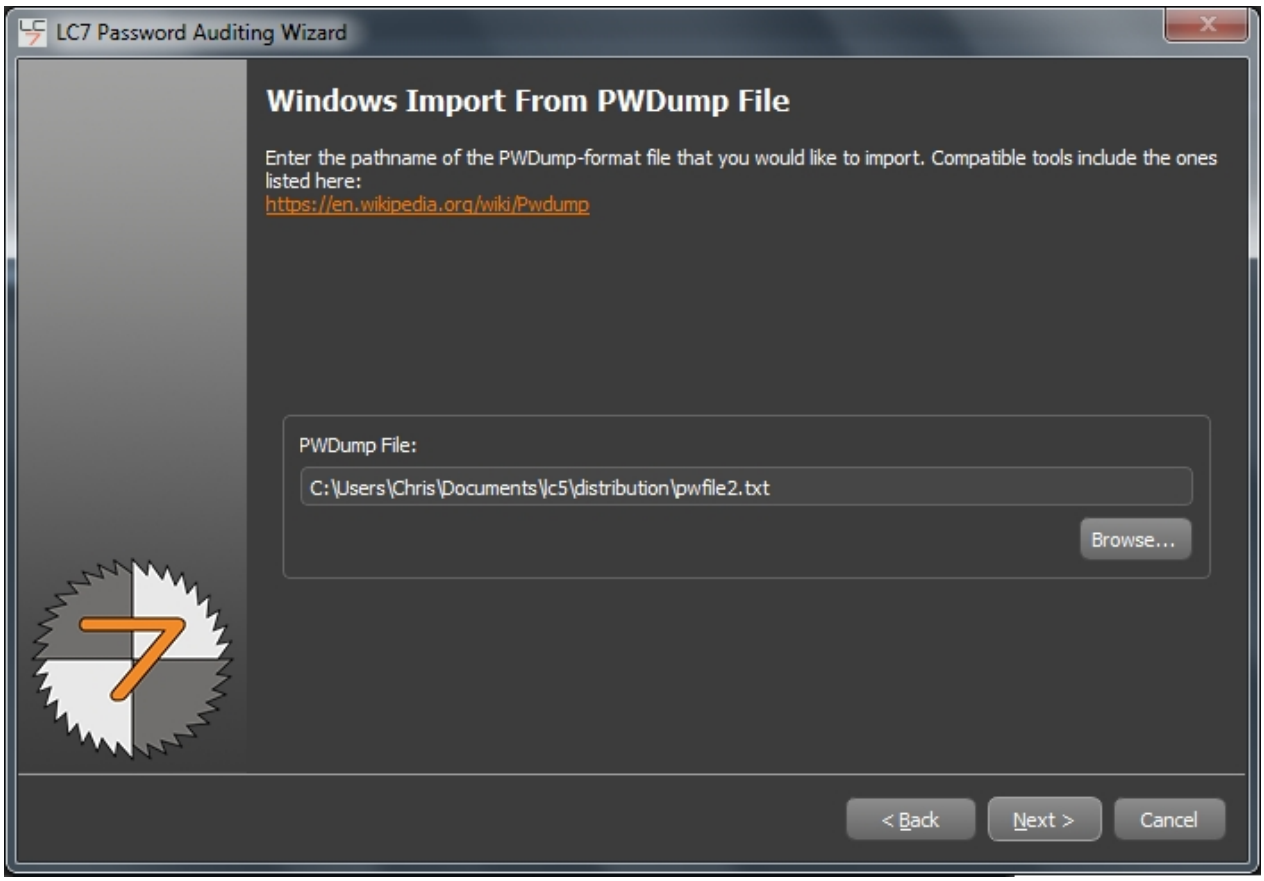
To extract password hashes from a remote machine via SMB you need admin privileges on the remote machine.

The SMB 'File and Print Sharing' service must be running on the remote machine.

If you are logged in with admin privileges for the remote machine you can select **Use Logged-In User Credentials**.
If you previously saved credentials for the remote machine you can select **Use Saved Credentials**.
If you are not logged in with remote machine privileges you can enter admin credentials by selecting **Use Specific User Credentials** and entering Username, Password, and Domain.
If you are entering in credentials you have the option to select **Save These Credentials** to save them in the Windows Protected Store for later usage with the **Use Saved Credentials** option.

Press **Next** to continue on to select audit type.

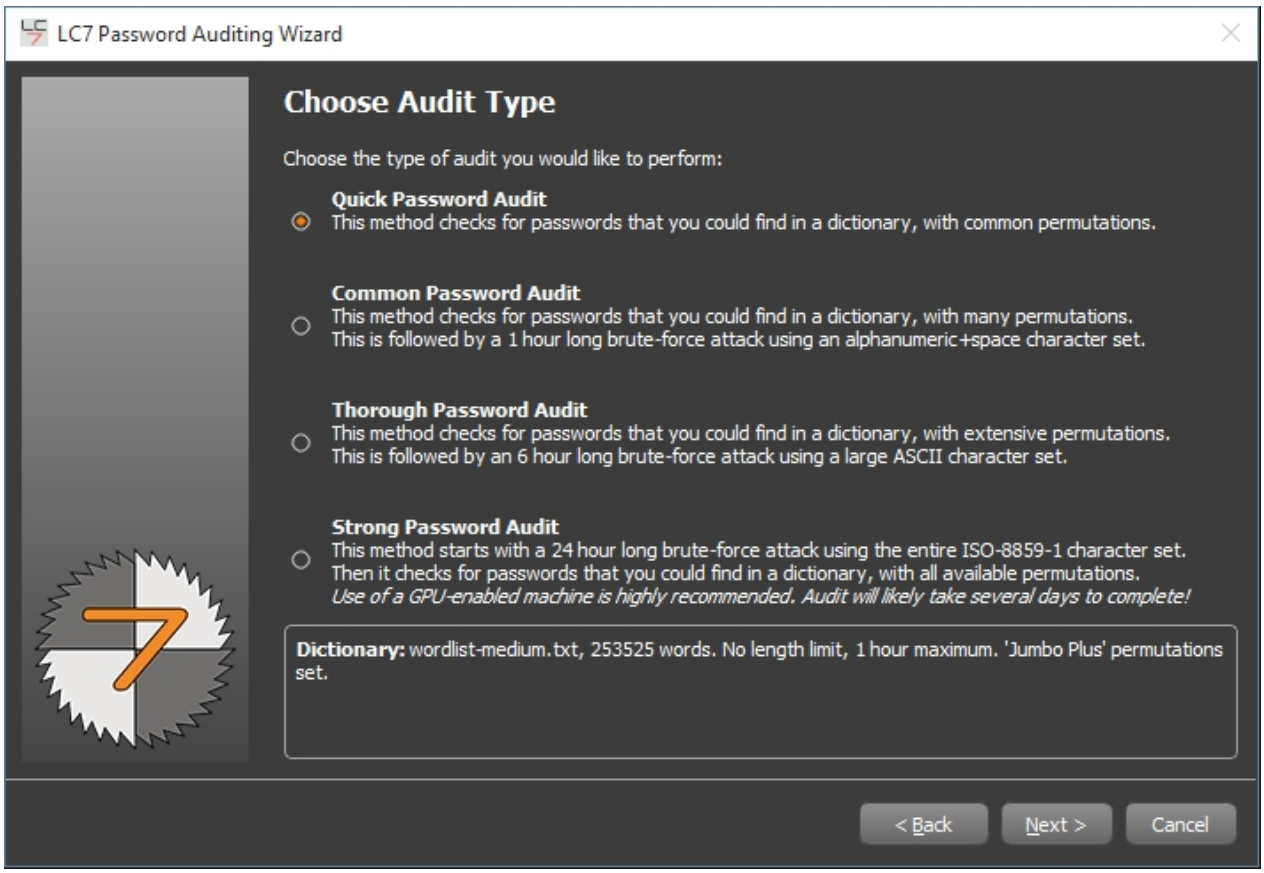
Windows Import From PWDump File



Click the **Browse** button and select the pwdump file you wish to import.

If you are uncertain of what tool to use to create a pwdump file, you can follow the provided link to a site about the Pwdump format, which will provide a list of compatible tools.
Once you have selected the correct file you can click **Next** to continue on to select audit type.

Choose Auditing Method



The L0phtCrack 7 wizard offers four different audit options. The more rigorous and involved the audit, the longer the audit requires.

- The Quick Password Audit takes up to an hour to perform and tries every word in a large dictionary file included with L0phtCrack 7 to find words matching the passwords you examine. It also tries common variations on those dictionary words.

- The Common Password Audit starts with the same dictionary attack as the Quick Audit, but with more extensive variations on the dictionary words. This is followed by a brute force attack that uses just the alpha-numeric character set (a-z, A-Z, and 0-9). It should take no more than 1 hours.

- The Thorough Password Audit uses a smaller word list for its dictionary attack segment, but with the more extensive word variations as well as common letter permutations, such as using '3' for 'e' and '$' for 's'. This is followed by a brute force attack using an expanded letters, number, and symbols character set. The total audit takes no more than 6 hours.

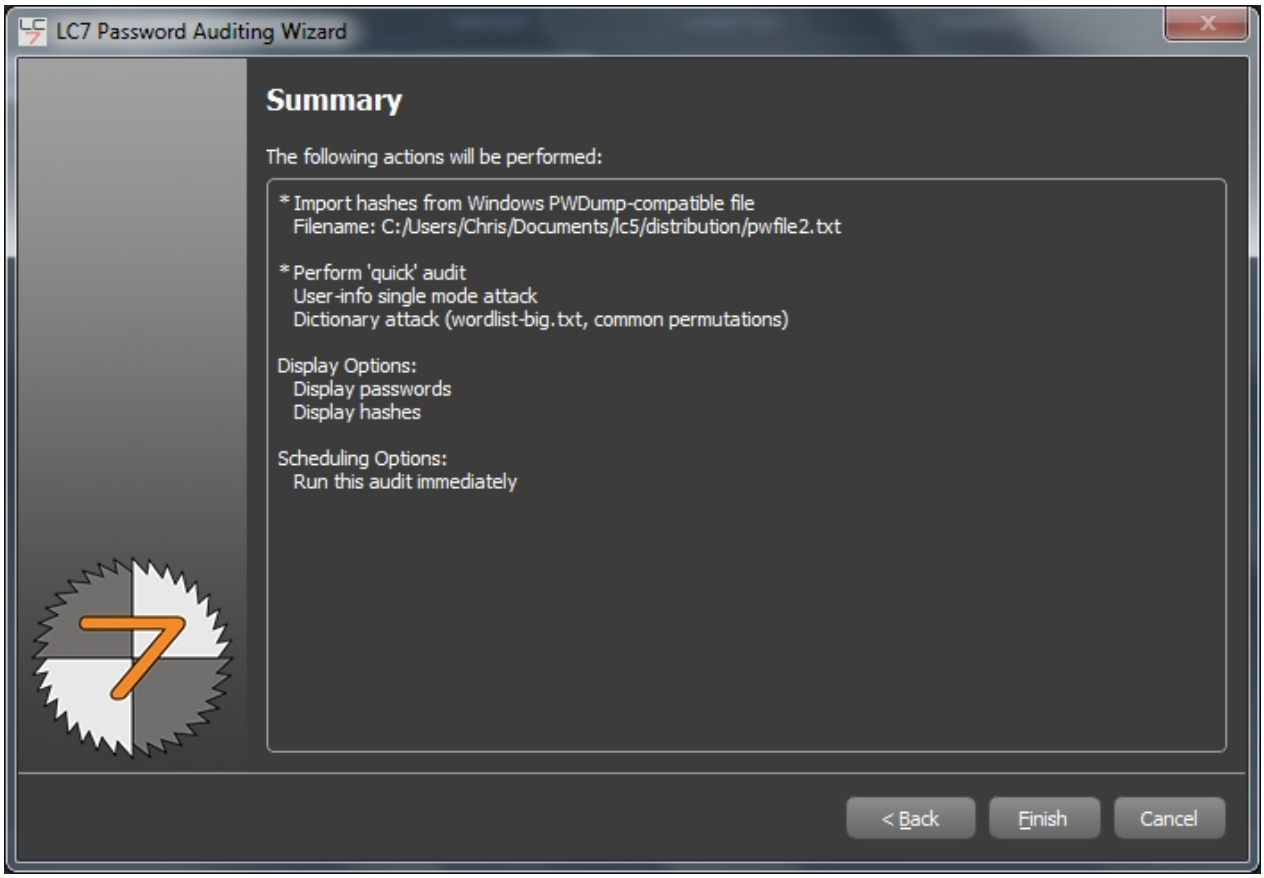
- The Strong Password Audit is more exhaustive, starting with a 24 hour brute force attack with the entire available ISO-8895-1 character set. After that it runs a dictionary attack using a large dictionary and all available permutations, with no time limit. For this mode, using a GPU is highly recommended as it may take several days to complete.

Pick Reporting Style

L0phtCrack 7 displays reports on what was found in the password audit. Choose the reporting style options to customize your report.

- Display passwords when audited causes cracked passwords to be displayed. Unselecting this box means reports show the safety of the password without disclosing the password itself.
- Display encrypted password hashes causes the encrypted version of the passwords to be included in the report.
- Display how long reports the length of time L0phtCrack 7 took to crack a password.
- Display auditing method reports the method used to find each password.
- Make visible notification when auditing is done displays an alert dialog when the audit completes, even if you're working in another application.

Begin Auditing



Once the Reporting options are selected, L0phtCrack 7 is ready to audit. Your settings are summarized before you finish. Click **Finish** to begin the password retrieval and audit process.

Using L0phtCrack 7

Passwords are sensitive information that can be used to impersonate users, including the operating system administrator.

For security reasons, operating systems do not store passwords in their original clear-text format. The original password cannot be derived directly from a hashed password. L0phtCrack 7 operates similar to a hacker to discover the password by automated guessing. Audits will start by guessing simple passwords that are based on simple variations on dictionary words, and progress to systematically trying all combinations of a set of characters. The amount of time it will take to crack a password varies with the password strength. Even with modern GPUs it can take a very long time to crack complex passwords.

L0phtCrack 7 obtains password hashes from the operating system, and then begins hashing possible password values. The password is discovered when there is a match between a target hash and a computed hash. L0phtCrack 7 must first import password hashes from the target system, and then uses various cracking methods to compute trial hashes. If there is a hash match we have retrieved the password.

Next:

Importing Password Hashes
How to get passwords hashes from your Windows and Unix systems into L0phtCrack 7 for auditing.

Configuring Audits
How to audit password hashes using Dictionary and Brute Force attacks.

Audit Progress And Status
Status and monitoring the progress of an auditing job.

Using Queues
How to use L0phtCrack's powerful batch queuing system to automate your regular auditing activities.

Scheduling Password Audits
Running a job in the future, or on a recurring basis.

Remediating Poor Passwords
Options to fix poor passwords right from the L0phtCrack user interface.

Reporting
Exporting information about your L0phtCrack 7 audits.

Settings
System settings and configuration options

Importing Password Hashes

Approaches to importing password hashes differ depending on where the password resides on the computer and your ability to access them.

L0phtCrack 7 can import password hashes directly from remote machines, from the local file system, from SAM, pwdump, or shadow files, and from Active Directory. Obtaining passwords over the network requires network access and administrator privileges to the target machine, as detailed below.

To begin the import process select **Import** from the **Passwords Menu Sidebar** on the left hand side of the main screen. When **Import** is selected you will see the main window display the **Import Mechanisms**. When you select an **Import Mechanism** you will see the right side of the main window change to a dialog for the inputs required such as file and machine names.

After you input the required filenames, hostnames and options for an Import Mechanism you will see the action buttons Run Import Immediately and **Add Import To Queue** ungray and become active. At this point you will likely press **Run Import Immediately** to perform the import action. Optionally you can press **Add Import to Queue** to build a queue. This is described in the Using Queues section below.

Next:

Import from Local Machine
For information on getting password hashes from the computer on which L0phtCrack 7 is installed.

Import from Remote Machine
For information on getting password hashes from another machine on your network.

Import from Unix/BSD/Solaris/AIX password/shadow File
To import Unix passwords hashes from a file on disk

Import from PWDump-style file
To import Windows password hashes from a file on disk

Import from SAM/SYSTEM files
To import Windows local user passwords from a registry backup

Import from NTDS.DIT/SYSTEM files

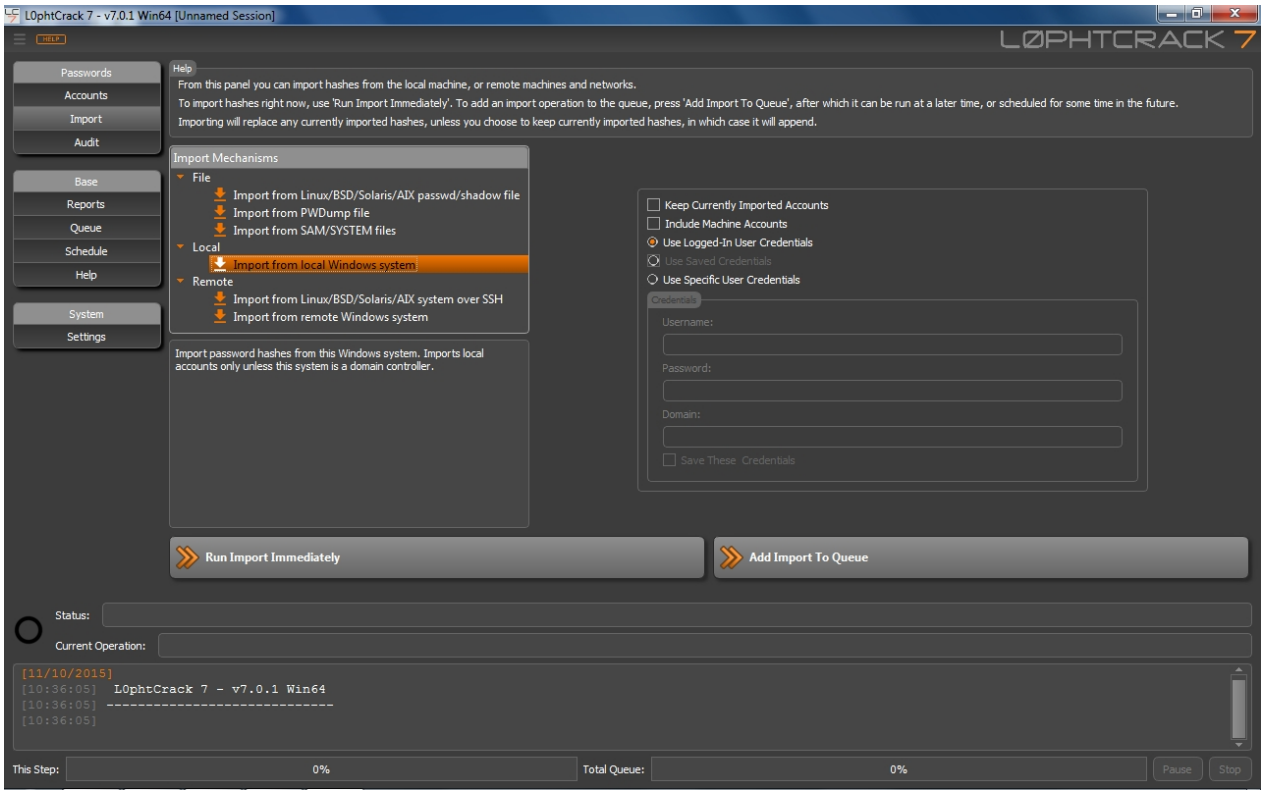
To import Windows domain passwords from a NTDS.DIT and SYSTEM registry backup

Import from Local Machine

To import password hashes from a local machine, you must be logged in with administrator rights or have an administrator/password pair. The local machine import works regardless of whether passwords are stored in a SAM file or in an Active Directory.

First, select Import from local Windows system. You can select to Keep Currently Imported Accounts if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. If you want to audit all system accounts, not just user accounts, you can select to Include Machine Accounts.

Next, specify the credentials that will be used to access the password hashes. You can choose Use Logged-In User Credentials. If you previously saved credentials for the local machine you can Use Saved Credentials. You can also select Use Specific User Credentials. If specific user credentials is selected you need to specify Username, Password, and optionally a Domain. You can select Save These Credentials to save the username, password, and domain to the Windows protected store for use in future audits. You are now ready to select your audit settings.



Import from Remote Machine

L0phtCrack 7 incorporates remote password hash retrieval, simplifying the process of obtaining password hashes, and reducing the need to use a third-party retrieval/dumping tool.

To import from remote machines select either Import from Linux/BSD/Solaris/AIX system over SSH if your target system is Unix-like or select Import from remote Windows system if your target system is Windows. Credentials with Root or Administrator privileges are required. If a security tool or some other element in the network environment is preventing remote hash retrieval, then you may have to use a third party tool to obtain the hashes and then follow the instructions for importing hashes from a pwdump file, SAM/System file (Windows), or shadow file (Unix).

Next:

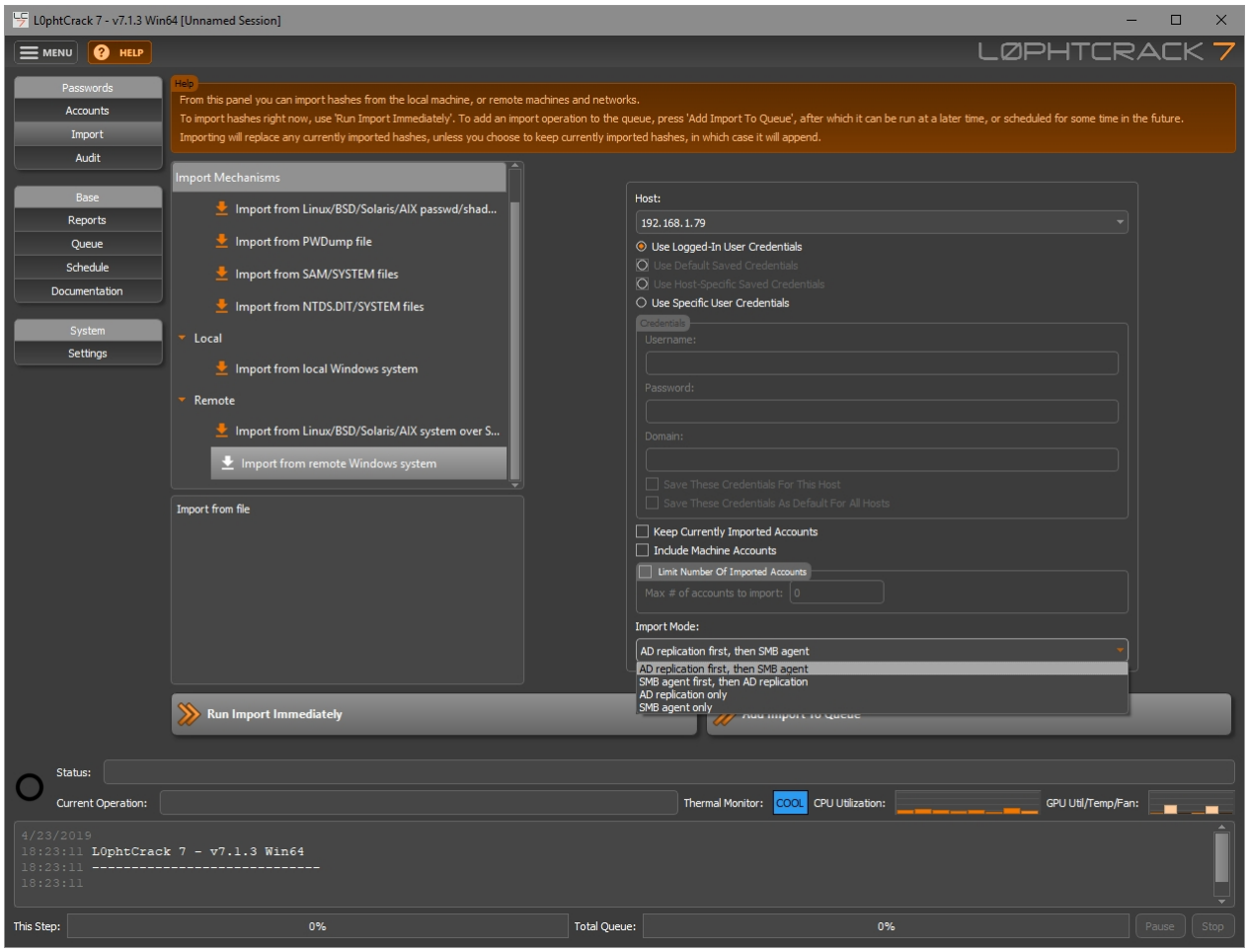
Windows
For importing from remote Windows systems

Unix
For importing from remote Unix systems

Windows

There are two available modes of operation for remote import from Windows machines

- AD Replication
- SMB Agent



AD Replication

To ease import from modern domain controllers (Windows 2008 and newer), you can use AD (Active Directory) Replication to do the hash import. This is preferable in many cases as it *does not require an SMB Agent to be installed on the domain controller.* Also, import can be performed by non-domain administrators if the account used for replication is given replication permissions. See the 'ADSI Edit' tool on the domain controller if you want to configure this.

SMB Agent

To import from non-domain controllers, or domain controllers for which AD Replication is not permitted or possible, one can use the 'classic' SMB Agent.
Windows SMB Agent remote importing requires SMB remote 'File And Print Sharing' to be enabled on the target machine, and for a remote agent program to be installed on the domain controller.

Configuration

Import mode can be set to one of the following:

- AD replication first, then SMB agent
- SMB agent first, then AD replication
- AD replication only
- SMB agent only

Using this setting you can control in what order each mechanism is attempted, or disable one of the import mechanisms if you do not wish to use it.

Specify the Host with either a name or IP address.

You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. If you want to audit all system accounts, not just user accounts, you can select to **Include Machine Accounts**.

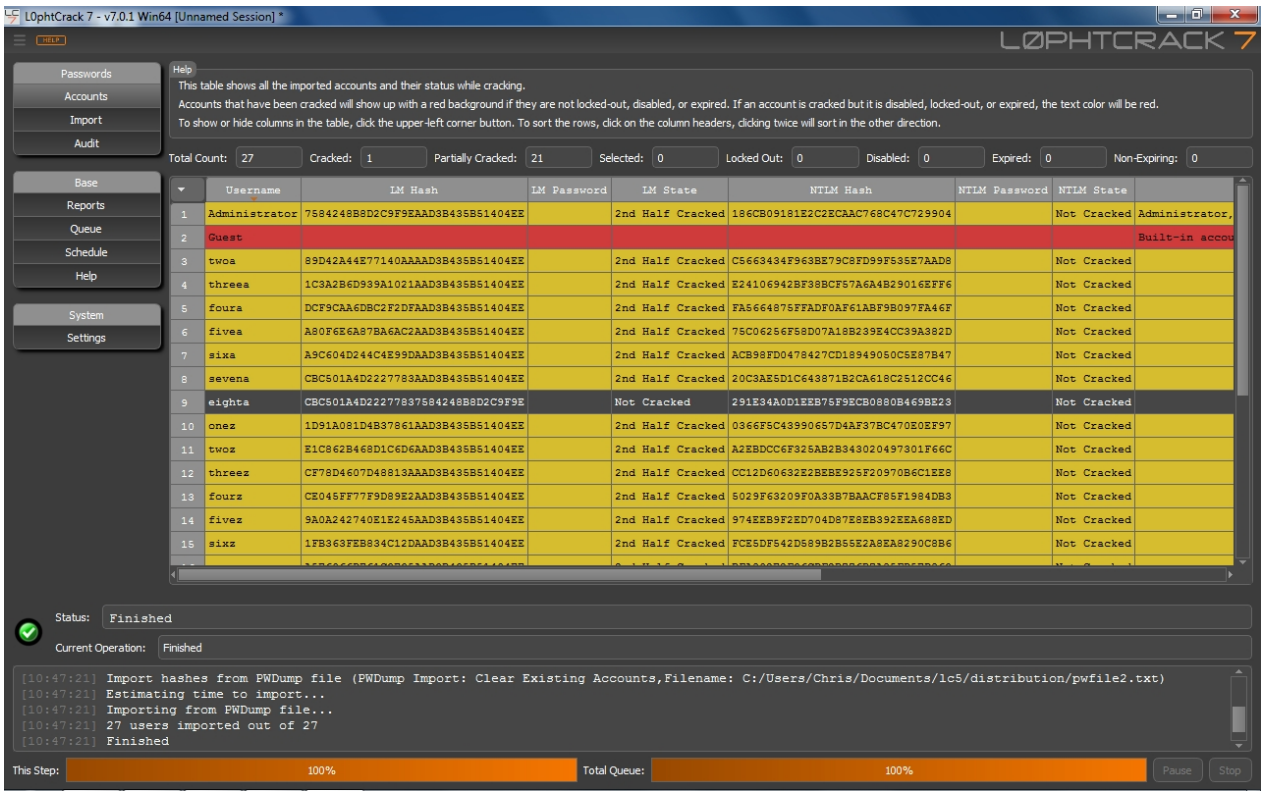
Next specify the credentials that will be used to access the password hashes. Credentials with administrative privileges on the target host are required.

You can choose to **Use Logged-In User Credentials**. Or, if you previously saved credentials you can choose **Use Default Saved Credentials** or **Use Host Specific Saved Credentials**.

You can also select **Use Specific User Credentials**. Next, you need to specify Username, Password, and optionally a Domain.

You can select **Save These Credentials For This Host** or **Save These Credentials As Default For All Hosts** to save the username, password, and domain to the Windows protected store.

Once you are satisfied with your import mechanism and import settings you need to press the **Run Import Immediately** button to perform the import. You can also select press the **Add Import to Queue** if you are creating a queue.
During the import the **Log Window** at the bottom of the screen will update and the password hashes will be displayed in the main window.



Remote Manual Installation of LC Agent

LC7 can automatically dump passwords remotely from other windows machines if you have file sharing enabled and administrator rights on the remote machine. However your configuration might require you to **manually** install the LC7 remote agent.

To manually install the LC Agent on a remote machine, follow the instructions below:

1. Select Generate Remote Agent in the MENU.

2. A warning dialog informs you that this process generates a public key and embeds it in the LC7 Remote Agent Installer.exe file. Browse to where you want to save the remote agent installer. Click Generate to create the remote agent.

3. Copy LC7 Remote Agent Installer.exe from your LC7 directory to the target machine.

4. Run the LC7 Remote Agent Installer.exe on the target machine. It will walk you through the installation process.

5. To remove the LC7 Remote Agent, go to the Control Panel, Programs and Features and Uninstall it.

6. Delete the LC7 Remote Agent Installer.exe file.

Unix

UNIX remote importing requires SSHD running on the target machine. Specify the **Host** with either a name or IP address and optionally a port number, if SSH isn't running on the default port 22.

Specify the port as follows: **hostname:port**

You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts.
You can also optionally select to **Include Non-Login and Disabled Accounts**.

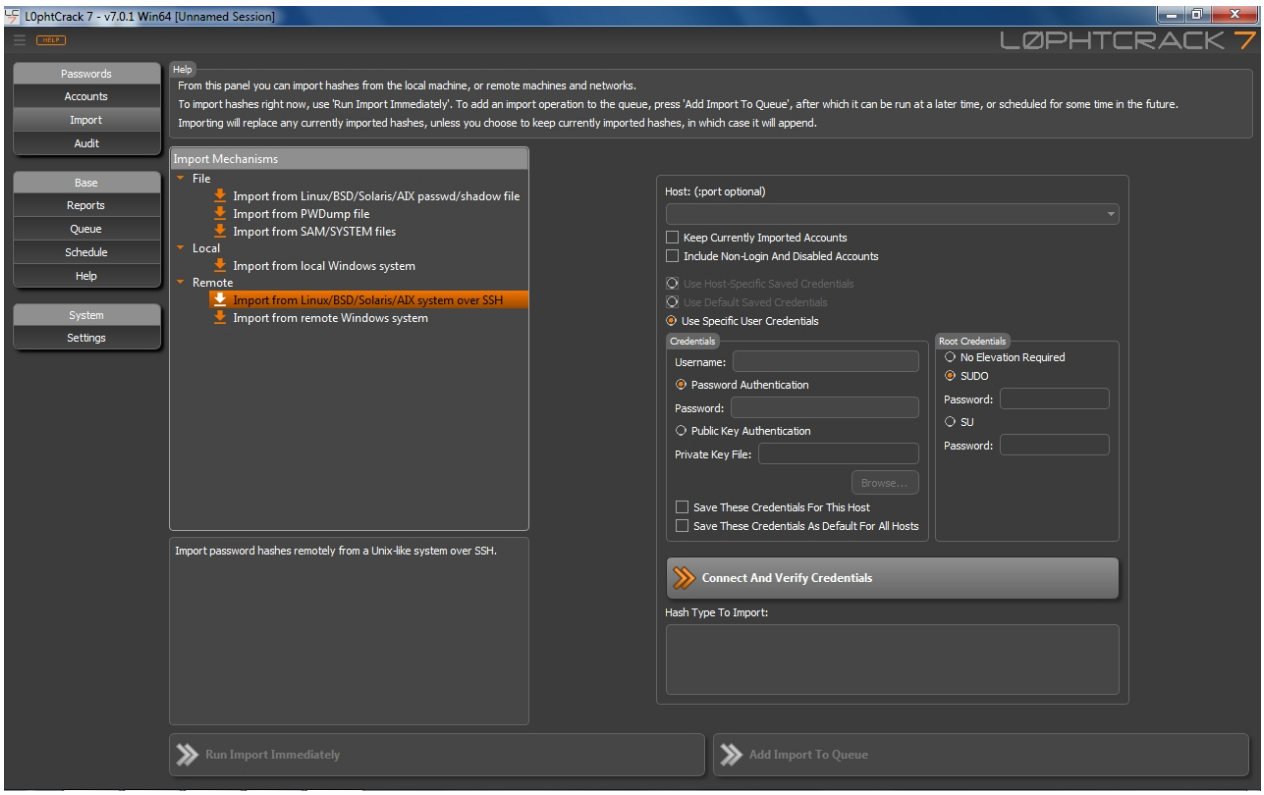
If you have previously saved credentials for this host you can use them by choosing **Use Host Specific Saved Credentials** or if you have previously saved default credentials for all Unix hosts you can use them by choosing **Use Default Saved Credentials**.

If you are not using saved credentials enter a **Username** and choose **Password Authentication** or **Public Key Authentication** and enter the appropriate secret, either a **Password** or **Private Key File**. If you are specifying user credentials, you can optionally select to save credentials for just this host and/or for all hosts by selecing the appropriate checkboxes. This will overwrite any previously saved credentials.

L0phtCrack requires root privileges to retrieve password hashes on a UNIX machine, but many SSH configurations will not allow a root user to log in. If this is the case, an additional root password will be required. If you specify credentials with root privileges choose **No Elevation Required**. If you specify non-root credentials you will need to choose either SUDO or SU based on what the target system uses to elevate privileges and enter a root password.

After you have specified host information, the credentials, and optionally a SUDO or SU password, press **Connect And Verify Credentials**. This will test that everything is correct for importing.

If the remote import parameters are correct you will see the Hash Type To Import list display the hash types found in the remote /etc/shadow and/or /etc/passwd file. L0phtCrack can only crack one type of Unix hash at a time so if there is more than one type select the one you wish to import. If you want to audit more than one type you will have to do the others in later sessions. You are now ready to select your audit settings.



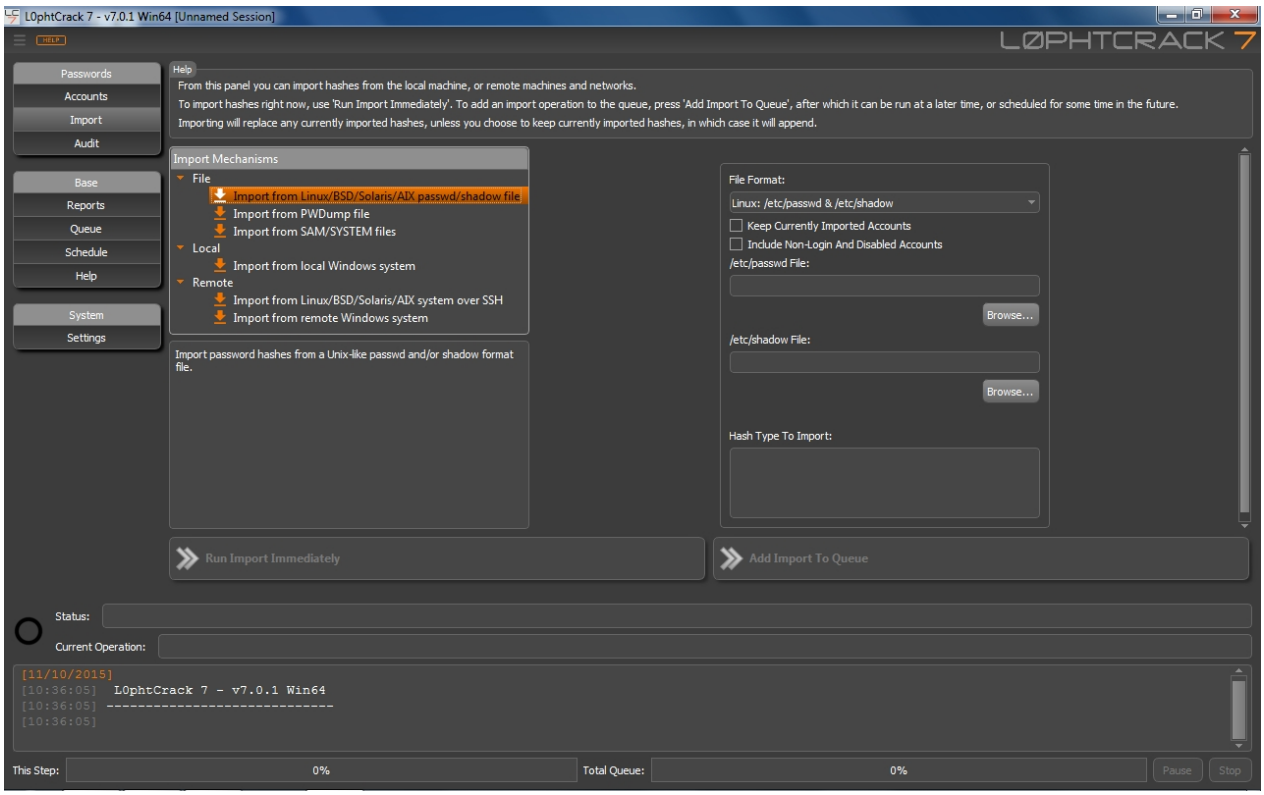
Import from Unix/BSD/Solaris/AIX passwd/shadow file

L0phtCrack 7 can extract Unix password hashes from the /etc/shadow file, which is where password hashes are usually found on a Unix system. L0phtCrack 7 can also extract user information from the /etc/passwd file. First select the **File Format** of the Unix system you are importing from.

For example, if the file came from a Linux system you'd select Linux: /etc/passwd & /etc/shadow. You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts.

You can also optionally select to **Include Non-Login and Disabled Accounts**. Next you use the **Browse** buttons to select the file(s) you wish to import. If you have chosen a **File Format** that has two files you are required to select the two files. L0phtCrack 7 can only crack a single Unix hash type at a time so if there are multiple hash types in the file you will need to select the type you want to crack. Only hashes of that type will be imported. You can then do the other hash types in later sessions.

You are now ready to select your audit settings.

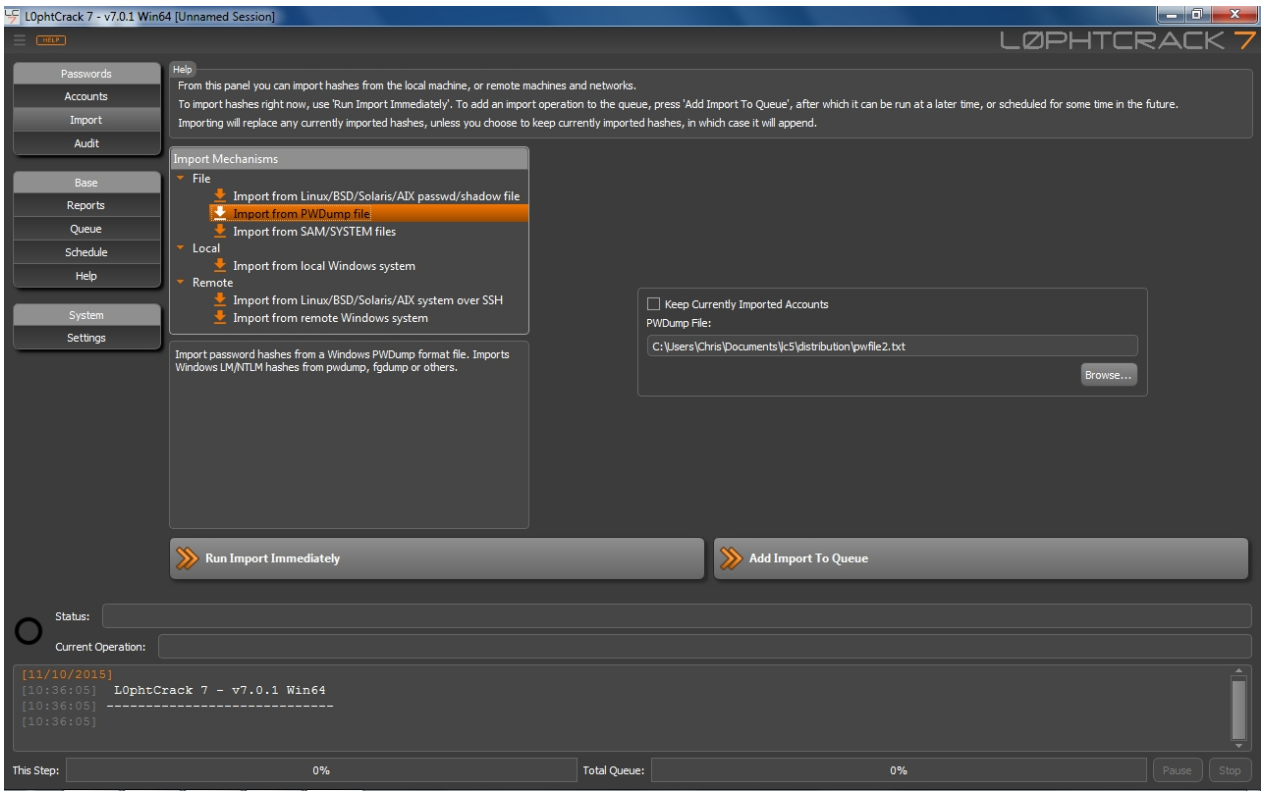


Import from PWDump-style file

PWDump files are created by tools that extract Windows password hashes from the Windows system. If the network or security tools in your environment prevent you from being able to connect to a remote machine to obtain the password hashes (or if the remote machine is on a different network), then you may need to use one of these tools to obtain a pwdump file of the hashes, and then import the hashes into L0phtCrack from that file.

Example tools are pwdump, pwdump3, fgdump, samdump, etc. If you have used one of these tools to create a PWDump file and you want to import the hashes, select **Import from PWDump** and browse to the file. You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts.

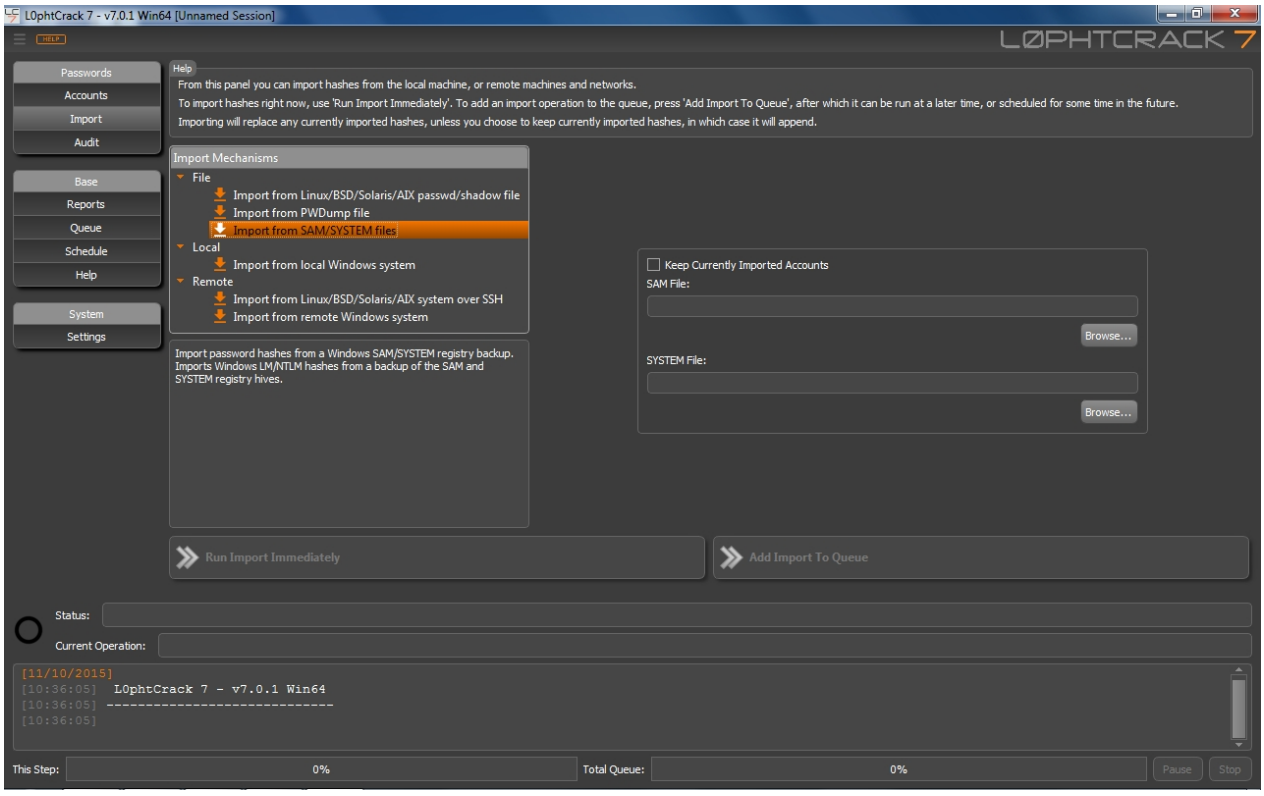
L0phtCrack 7 can usually import hashes directly from the local machine or a remote machine so in those cases you can follow the local and remote instructions below to perform those types of imports. You are now ready to select your audit settings.



Import from SAM/SYSTEM files

You can import password hashes from a Windows SAM/SYSTEM registry backup.

Browse to the SAM file and then **Browse** to the SYSTEM file. You must specify both files. You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. You are now ready to select your audit settings.



Import from NTDS.DIT/SYSTEM files

You can import domain password hashes from a Windows NTDS.DIT/SYSTEM registry backup. These files are typically retrieved by copying the files from a volume shadow copy. If you have already acquired an NTDS.DIT and SYSTEM file the appropriate way, skip to the next section. If you haven't done this before successfully using other tools, you may want to read these instructions on preparing the files correctly for import, as it is easy to get a corrupted database if you copy it incorrectly.

Preparing NTDS.DIT and SYSTEM for Import

NTDS.DIT, the active directory database, is locked while the domain controller is running, which means you can't just copy it.

You have two options here, one is 'offline dumping', which takes the domain controller offline for the duration of the operation, but guarantees an accurate dump, and the other is 'online dumping' which copies the database but possibly doesn't get the entire thing, because some operations may not be fully committed at the time of the snapshot. Specifically, AD operations performed since the last reboot may not be captured. Offline dumping is preferred for systems older than Windows Server 2008. The Online dumping process for Server 2008 and newer is preferred.

ONLINE DUMPING (WINDOWS SERVER 2008 and newer)

To pull the NTDS.DIT and SYSTEM files from the running domain controller:

1. 'Run As Administrator' cmd.exe to get an administrator command shell

2. In that command shell run:

```
cd /d %TEMP%
mkdir ntdscopy
cd ntdscopy
ntdsutil "activate instance ntds" "ifm" "create full ." "quit" "quit"
esentutl /d "Active Directory\ntds.dit"
```

3. Take this 'ntdscopy' folder and copy it to the machine you're running L0phtCrack on, and use the Import NTDS.DIT/SYSTEM option to import the two files, 'NTDS.DIT' and 'SYSTEM'.

OFFLINE DUMPING

To pull the NTDS.DIT, you should restart the domain controller in directory services restore mode. If you need to reset the 'DSRM Password', follow these instructions:

https://support.microsoft.com/en-us/kb/322672

To restart the server in DSRM mode, follow these instructions (based on https://technet.microsoft.com/en-us/library/cc794729%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396) (These instructions assume Windows is installed in C:\Windows\ and the NTDS files are in C:\Windows\NTDS):

1. 'Run As Administrator' cmd.exe to get an administrator command shell
   At the command prompt, type the following command, and then press ENTER:

```
bcdedit /set safeboot dsrepair
```

2. At the command prompt, type the following command, and then press ENTER:

   ```
   shutdown -t 0 -r
   ```

   The domain controller restarts in Directory Services Restore Mode. If you are connected over RDP when the domain controller restarts, your Remote Desktop Connection is dropped. Wait for a period of time that is adequate for the remote domain controller to restart, and then open Remote Desktop Connection.

3. The domain controller name should still be showing in Computer. If it is not, select it in the list, and then click Connect.
   In the Windows Security dialog box, click Use another account.

   In User name, type the following:
   `MachineName\Administrator`
   Where MachineName is the name of the domain controller.

4. In Password, type the Directory Services Restore Mode password, and then click OK.
5. At the logon screen of the remote domain controller, click Switch User, and then click Other User.
6. Type `MachineName\Administrator`, and then press ENTER.
7. Once logged in open an administrative command prompt and type the following commands:

   ```
   cd %TEMP%
   mkdir ntdscopy
   cd ntdscopy
   copy c:\windows\ntds .
   reg save HKLM\SYSTEM SYSTEM
   ```

8. Take this 'ntdscopy' folder and copy it to the machine you're running L0phtCrack on, and use the Import NTDS.DIT/SYSTEM option to import the two files, 'NTDS.DIT' and 'SYSTEM'.
9. To return to normal operation, take the system out of DSRM, by running the following commands in the administrative command prompt:

   ```
   bcdedit /deletevalue safeboot
   shutdown -t 0 -r
   ```

ONLINE DUMPING (PRE-WINDOWS SERVER 2008)

To pull the NTDS.DIT and system from a running domain controller, assuming Windows is installed in C:\Windows\ and the NTDS files are in C:\Windows\NTDS:

1. 'Run As Administrator' cmd.exe to get an administrator command shell

2. In that command shell, run: (substitute c: for whatever drive Windows and the NTDS folder is installed on)

   ```
   vssadmin create shadow /for=c:
   ```

3. Note the 'Copy ID' and 'Volume Name' in the command output, it looks like this:

   ```
   vssadmin 1.1 – Volume Shadow Copy Service administrative command-line tool
   (C) Copyright 2001 Microsoft Corp.
   Successfully created shadow copy for ‘c:\’
   Shadow Copy ID: {..guid..}
   Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
   ```

4. Switch to a temporary directory, and make a folder to work in:

```
cd /d %TEMP%
mkdir ntdscopy
cd ntdscopy
```

5. Copy the NTDS.DIT and EDB files from the C:\Windows\NTDS folder: (substituting in the 'Volume Name' from above if different)

   ```
   copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\* .
   ```

6. Repair the NTDS.DIT since it was copied while it was still opened:

   ```
   esentutl /p ntds.dit
   ```

7. Copy also, the SYSTEM registry hive, because you'll need that to decrypt the NTDS.DIT data.

   ```
   reg save HKLM\SYSTEM SYSTEM
   ```

8. Take this 'ntdscopy' folder and copy it to the machine you're running L0phtCrack on, and use the Import NTDS.DIT/SYSTEM option to import the two files, 'NTDS.DIT' and 'SYSTEM'.

9. Remove the volume shadow copy if you would like with either one of these two commands: (if you have no other volume shadow copies)

   ```
   vssadmin delete shadows /for=c:
   ```

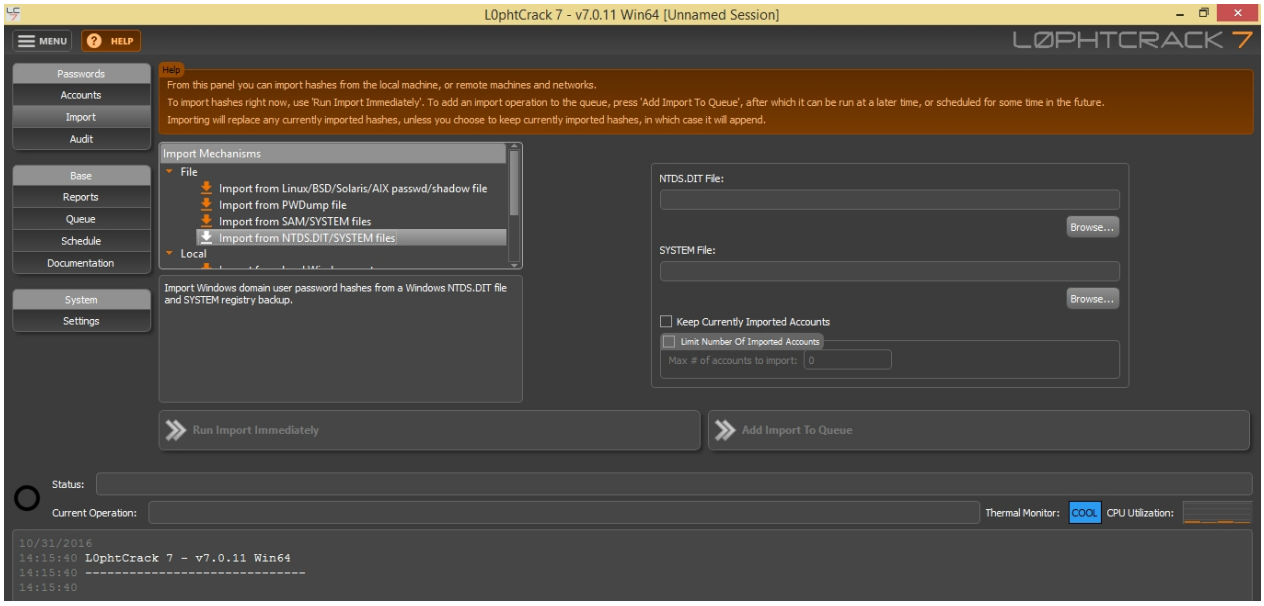
10. (if you want to delete just the specific shadow copy you just created, substituting the 'Copy ID' from above for '{..guid..}')

    ```
    vssadmin delete shadows /shadow={..guid..}
    ```

Importing the NTDS.DIT and System Files

Browse to the NTDS.DIT file and then **Browse** to the SYSTEM file. You must specify both files. You can select to **Keep Currently Imported Accounts** if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. You can also set a limit on the number of accounts to import.

You are now ready to select your audit settings.



Configuring Audits

The cracking processes that generates password values provides several options that balance audit rigor against the time required to crack. Effective auditing, therefore, requires an understanding the underlying business goals, and the security thresholds necessary to meet them.

The difference between the strengths of weak versus strong passwords demonstrates the value of strong passwords in protecting your organization or machine. Using a real-world password auditing tool helps discover the strength of passwords in your organization, and determine:

- Whether users are following password policies,
- The compliance rate or non-compliance instances with such policies,
- The effectiveness of a password filter, or
- Password expiration times.

L0phtCrack 7 includes three Audit Techniques: User Info, Brute Force, and Dictionary. To begin the Audit process select **Audit** from the **Passwords Menu Sidebar** on the left hand side of the main screen. When **Audit** is selected you will see the main window display the **Audit Techniques**. When you select an **Audit Technique** you will see the right side of the main window change to a dialog for the inputs required such as length and character set.
There are three included audit techniques. You must select one of:

- User Info - uses username and user full name as passwords
- Dictionary - uses words in a wordlist with permutations as passwords
- Brute Force - exhaustive attempts using all characters in a character set up to a specified password length

After you choose an audit technique and select a preset you will see the action buttons **Run Audit Immediately** and **Add Audit To Queue** un-gray and become active. If you want to import hashes and audit them right away, click **Run Import Immediately** to perform the audit action. If you want to schedule the import action for later, you can instead click **Add Import to Queue** to build a queue. This is described in the Using Queues section.

Next:

User Info
Audit using username and user full name as passwords

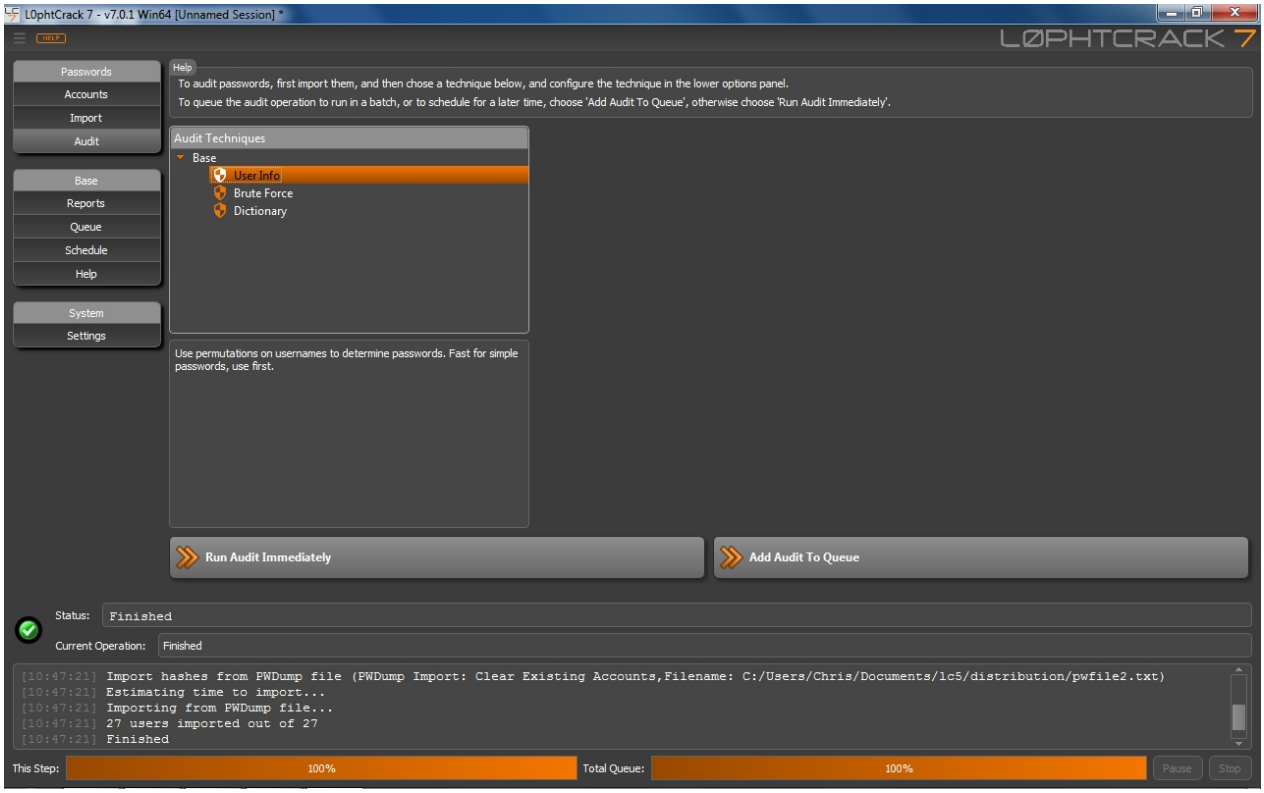
Dictionary
Audit using words in a wordlist with permutations as passwords

Brute Force
Audit using exhaustive attempts using all characters in a character set up to a specified password length

User Info Crack

L0phtCrack 7 first checks to see if any accounts have used the username as a password. These are weak passwords that you need to know about right away. This crack is performed first in every audit, because it is very quick. There are no options to select.

If you have already imported the password hashes to audit and you are satisfied with your audit technique and configuration, press the **Run Audit Immediately** button to begin your audit.



Dictionary Crack

The next fastest method for retrieving simple passwords is a dictionary crack. L0phtCrack 7 tests all the words in a dictionary or wordfile against the password hashes. It also permutes the words with the characters users often substitute, prepend or append to words when creating passwords. Once L0phtCrack 7 finds a correct password, the result is displayed.

L0phtCrack 7 includes four wordlist files of increasing size: **wordlist-small.txt, wordlist-medium.txt, wordlist-large.txt, wordlist-huge.txt**. The word list files are text files with one word per line, so they are easy to customize. We recommend doing so, or adding an additional word list, so that you can include your organization name, local team names, or any other words or names specific to your organization and

location that users might be basing passwords off of.

The wordlist files and permutation types are specified in a dictionary crack preset which is selected from the **Preset** list. When you select a preset you will see the configuration of the preset in the **Preset Configuration** to the right of the preset list. The configuration is grayed out unless you are editing the preset.

There are four included presets:

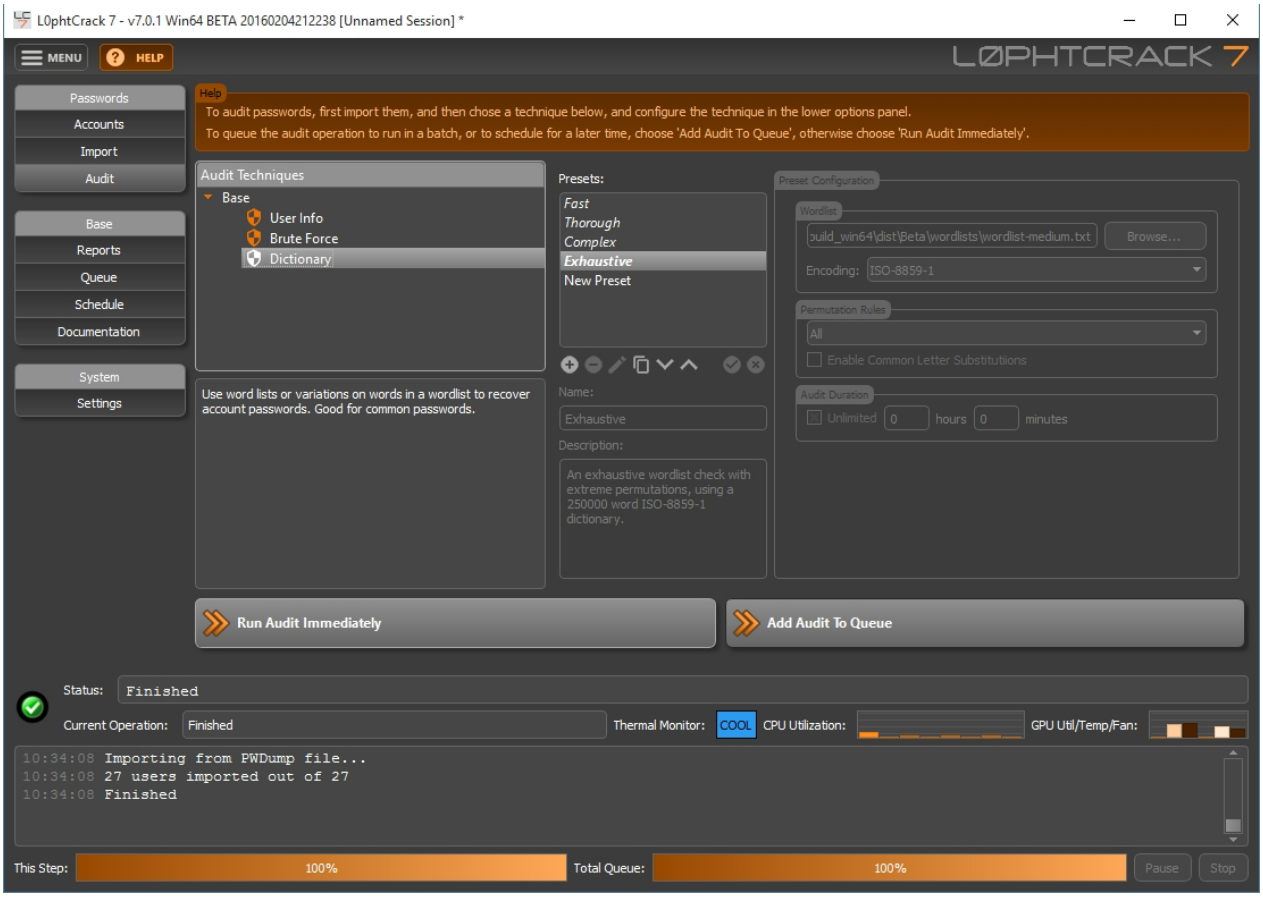
- Fast - **wordlist-medium.txt** with **Jumbo Plus** permutation rules, for **Audit Duration** of 1 hour
- Thorough - **wordlist-medium.txt** with **Wordlist Plus** permutation rules, and **Common Letter Substitutions** for **Audit Duration** of 6 hours
- Complex - **wordlist-small.txt** with **Jumbo** permutation rules, and **Common Letter Substitutions** for **Audit Duration** of 24 hours
- Exhaustive - **wordlist-medium.txt** with **All** permutation rules, for **Audit Duration** of Unlimited

Below the **Presets** list is a set of buttons that are used to create a preset, remove a preset, edit a preset, and duplicate a preset.

To create a new preset press the + button and then add a name and description. In the **Preset Configuration**, select a **Wordlist**, an **Encoding**, the **Permutation Rules**, and a **Duration**. When you are satisfied with your settings press the checkmark button to save the preset.

You may also duplicate the included presets and modify the duplicate. You cannot edit or remove the included presets. They are displayed in an italic font.

If you have already imported the password hashes to audit and you are satisfied with your audit technique and configuration, press the **Run Audit Immediately** button to begin your audit.



Brute Force Crack

The most comprehensive cracking method is the brute force method, which recovers passwords of any length and any characters, even a completely random string if it isn't too long.

The brute force crack attempts every combination of characters it is configured to use. Your choice of character sets determines how long the brute force crack takes. Short, common passwords, based on letters and numbers can typically be recovered in about a day using the default character set A-Z and 0-9. Longer or more complex passwords, on the other hand, that use characters such as #_}* could take a very long time to crack on the same machine depending on the length of the password. Passwords for all systems except LANMAN on Windows are case-sensitive. L0phtCrack 7 tries both upper and lower case characters.

Password Length, **Audit Duration** and **Character Set** are specified in a **Brute Force** preset which is selected from the **Preset** list. When you select a preset you will see the configuration of the preset in the **Preset Configuration** to the right of the preset list. The configuration is grayed out unless you are editing the preset.

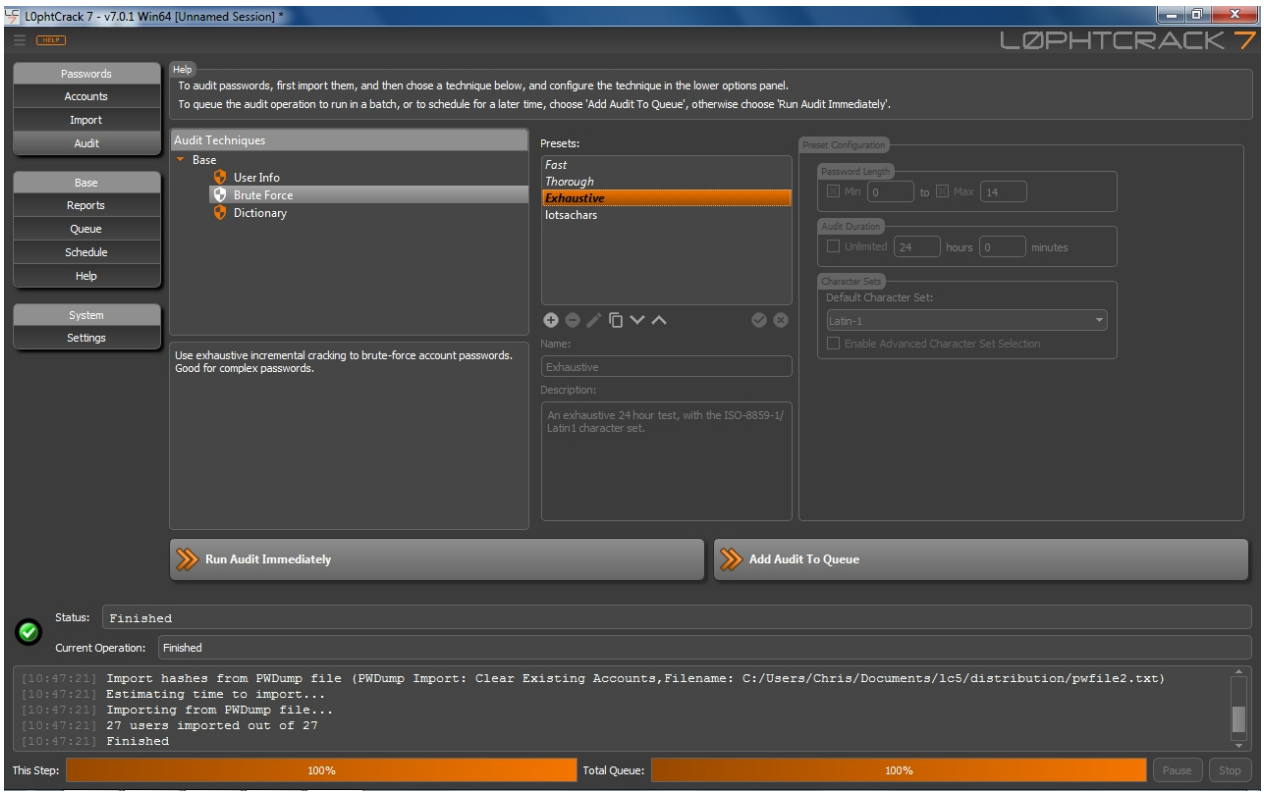
There are three included presets:

- Fast - **Password Length** of 7 with **Audit Duration** of 1 hour and **Character Set** of Alphanumeric + Space
- Thorough - **Password Length** of 10 with **Audit Duration** of 6 hours and **Character Set** of ASCII
- Exhaustive - **Password Length** of 14 with **Audit Duration** of 24 hours and **Character Set** of Latin-1

Below the **Presets** list is a set of buttons that are used to create a preset, remove a preset, edit a preset, and duplicate a preset.

To create a new preset press the + button and then add a name and description. In the **Preset Configuration**, specify a **Password Length**, an **Audit Duration**, and a **Character Set**. When you are satisfied with your settings press the checkmark button to save the preset. You may also duplicate the included presets and modify the duplicate. You cannot edit or remove the included presets. They are displayed in an italic font.

If you have already imported the password hashes to audit and you are satisfied with your audit technique and configuration, press the **Run Audit Immediately** button to begin your audit. You can optionally press the **Add Audit to Queue** if you are creating a queue.



Audit Progress and Status

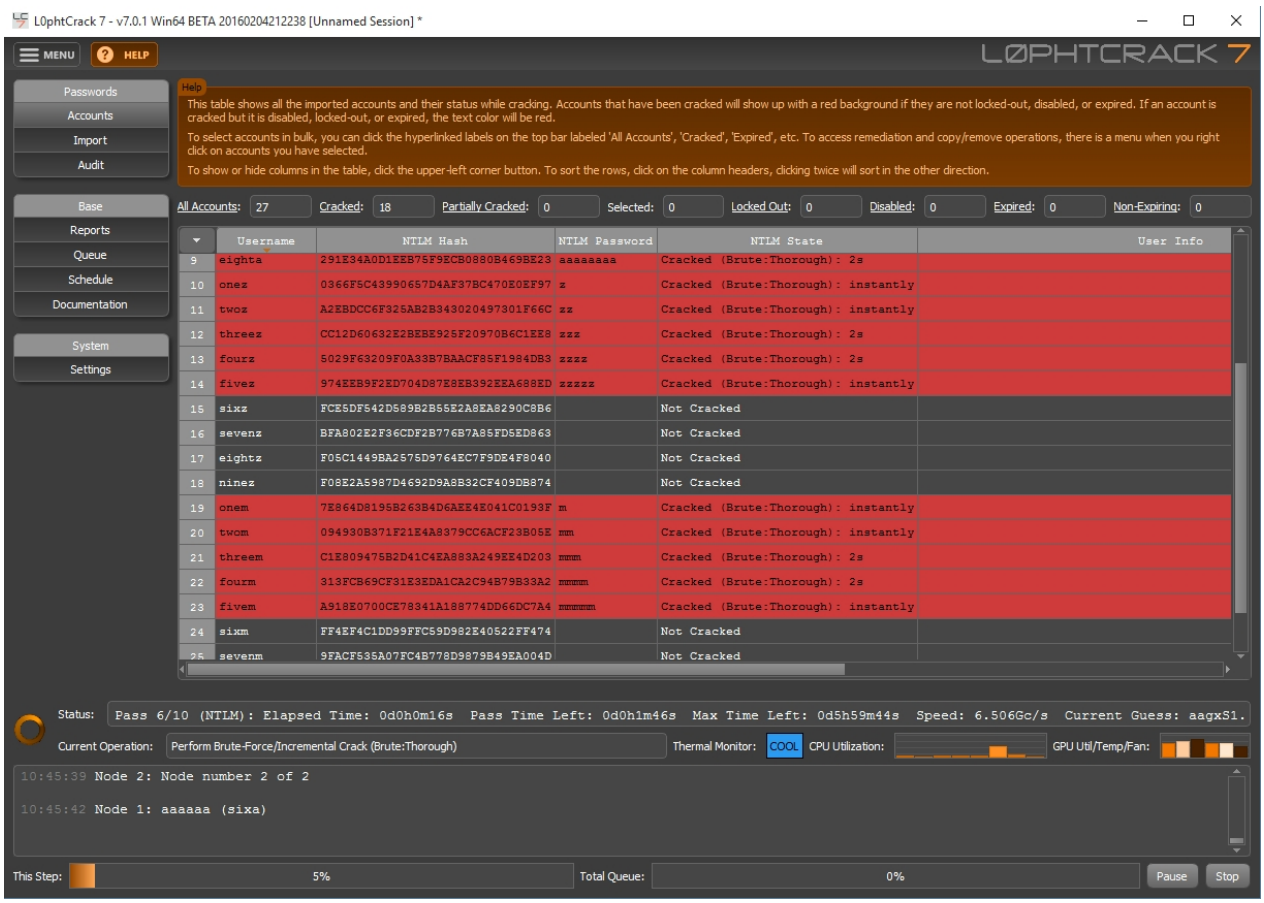
Once you begin the **Audit** the main window will display the imported password hashes and show the progress of the auditing session. A row consists of a username, the hash, the password if cracked, the state of the password cracking, user info, user id, the last time the account was changes, and if the account is locked, if disabled, password expiration or if no expiration. Rows will be colored red when a password is cracked, including if there is no password. Rows are yellow if there if a partial crack (with LANMAN hashes it is possible to crack just half of the password).

The **Status** windows will display whether the auditing session is in progress or not. The log window will log operations such as when a particular auditing type begins and when passwords were cracked. The progress bars display the percentage complete for a audit step and the total work queue.

You can **Pause** or **Stop** the audit session using the **Pause** and **Stop** buttons in the lower right of the main window. If the audit session is paused you can **Resume** with the **Resume** button.

The **Thermal Monitor** displays the temperature of the CPU and GPU. **CPU Utilization** displays the a bar for each core or hyperthread. The height of the bar represents utilization from 0 to 100%. The **GPU Util/Temp/Fan** displays the percentage of GPU utilization, the GPU temp, and the Fan speed. There is a bar for each GPU found in the system.

L0phtCrack automatically throttles your GPU if it begins to overheat. The temperature settings are available in the **Settings** menu on the **System Sidebar Menu**.



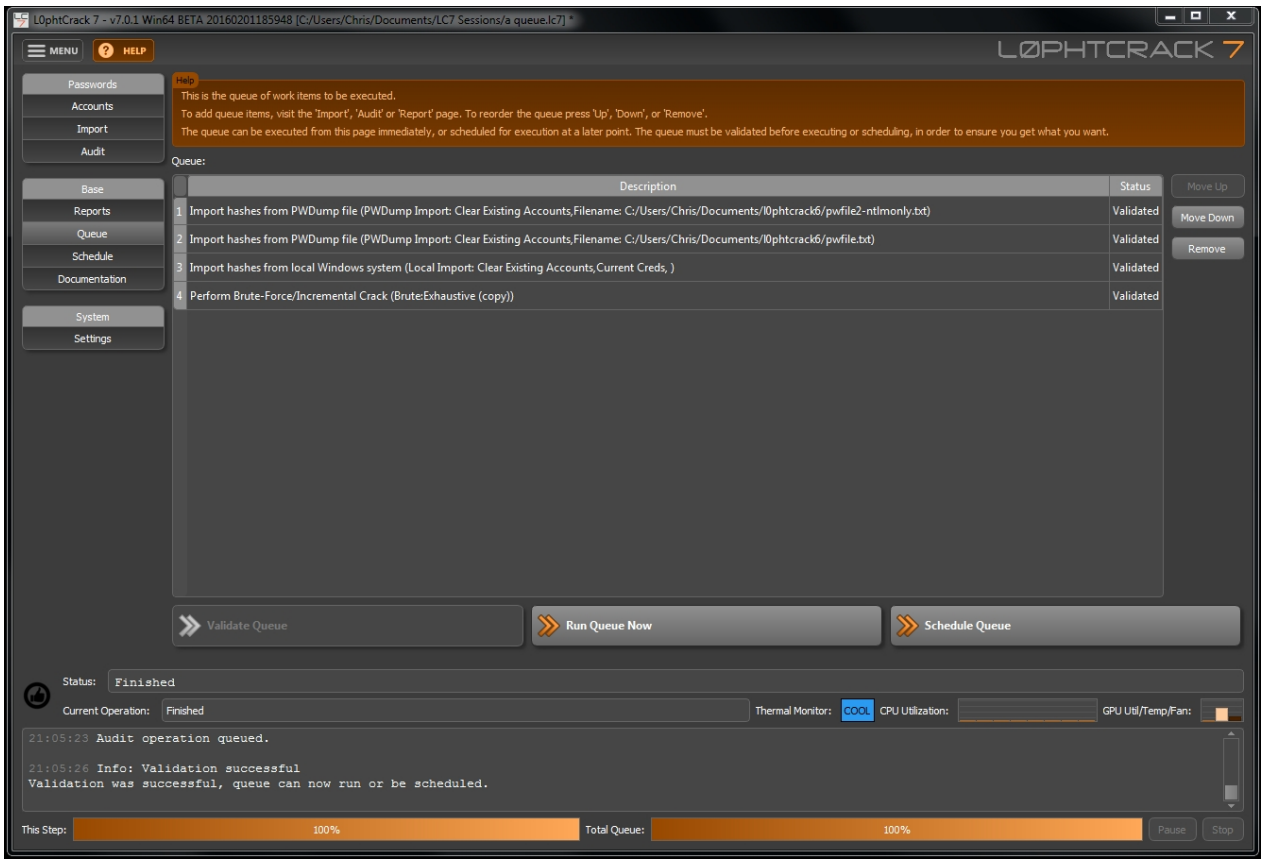
Using Queues

L0phtCrack 7 contains a powerful queue feature which lets you string multiple import and audit operations together. You can then run the queue immediately or choose to schedule the queue. This way you can schedule complex import and auditing functions to occur on a schedule. For instance, you could set up a queue to import password hashes from multiple machines and then run an audit on the passwords on a repeating schedule. This is an easy way to perform a monthly audit.

Whenever you use the password import function you can choose **Add Import To Queue** instead of **Run Import Immediately**. This will place the import on the **Queue**. Remember to select **Keep Currently Imported Accounts** during import if you want to concatenate many imports together for one auditing session. When you are on the audit selection you can choose to **Add Audit To Queue** instead of **Run Audit Immediately** to put that audit action on the **Queue**.

When you select **Queue** on the right hand menu the **Queue** window displays all the items that have been added to the queue. Before you run of schedule the **Queue** you need to **Validate Queue**. This checks for any errors that may prevent the **Queue** from running. If the validation succeeds the **Run Queue Now** and **Schedule Queue** buttons become enabled. See Scheduling Password Audits for a description of how to schedule audits.

The queue is saved with the session in the .lc7 file. If you choose **Save Session** not only will you save any imported password hashes and their audit state, you will also save the **Queue**.

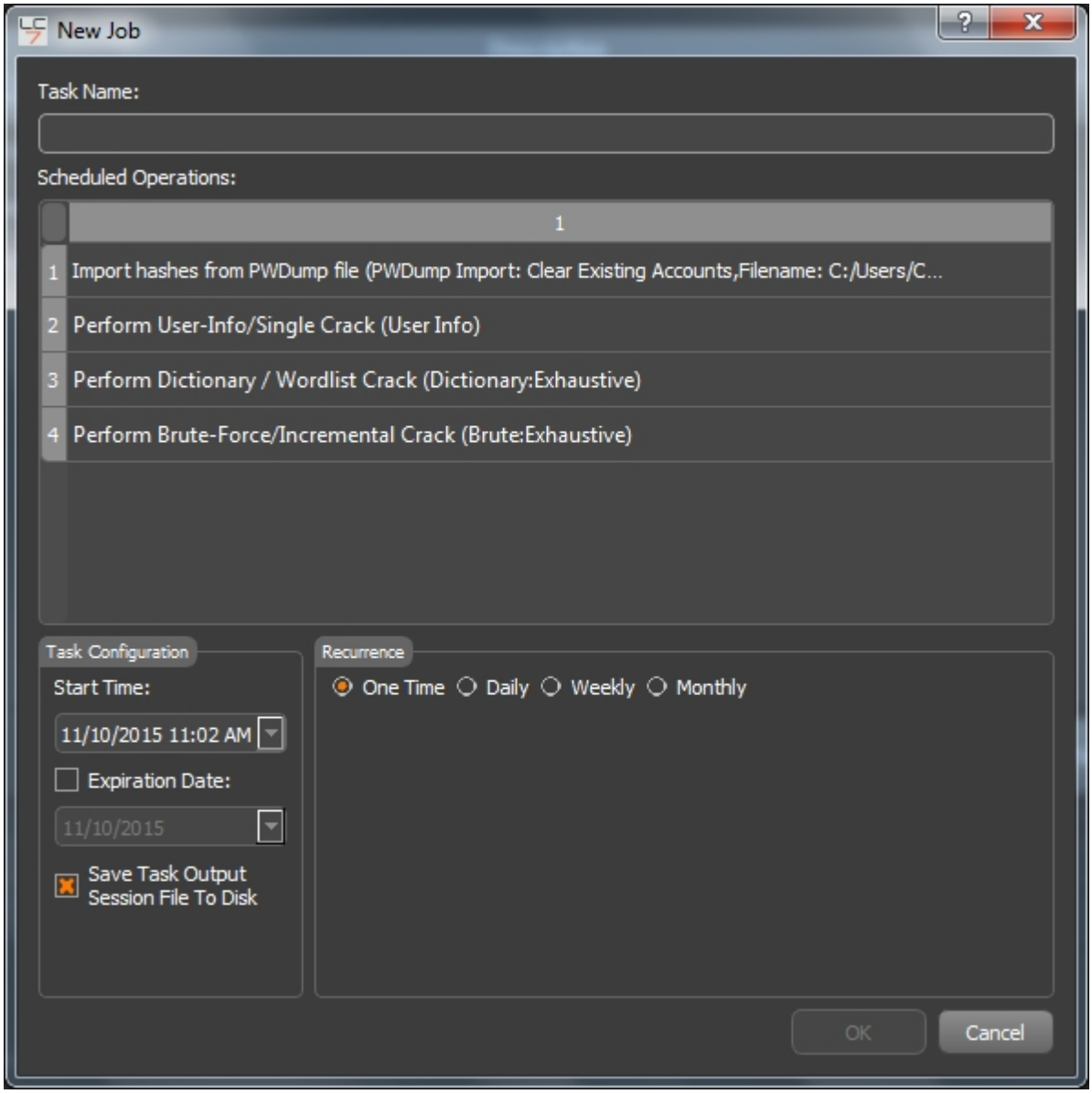


Scheduling Password Audits

Administrators can schedule audits daily, weekly, monthly, or just once. This allows you to perform recurring audits on a set schedule without needing to manually import and audit hashes each time.

To schedule a task, first create a **Queue** with a set of imports and audits by using the **Add Import To Queue** from the import window and **Add Audit to Queue** from the audit window.

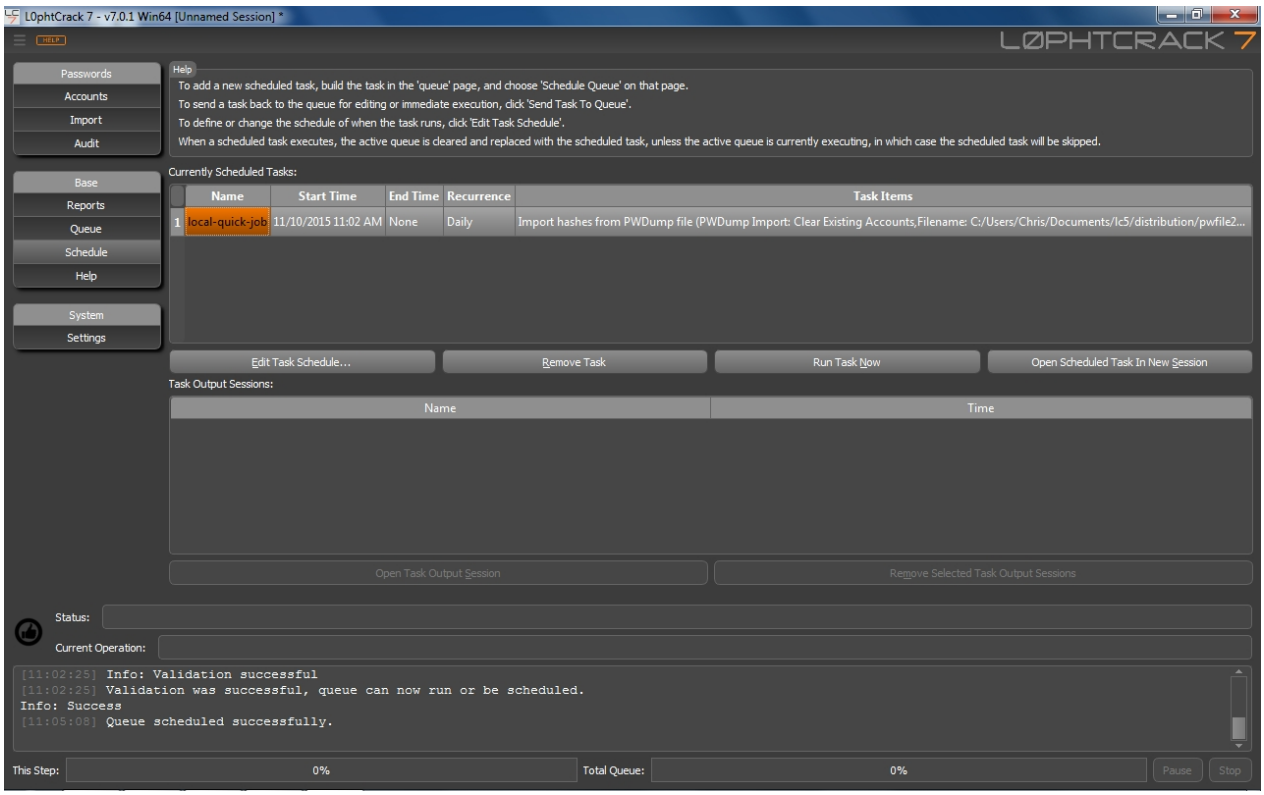
Next, select **Queue** from the left side menu to display the queue window. Instead of running the queue press the **Schedule Queue** button. The **New Job** dialog will display. You will see the tasks in the queue. You can now set a **Start Time** and optionally an **Expiration Date**. You can also set a **Recurrence** interval of **One Time, Daily, Weekly, Monthly**. When you are satisfied with the settings press the **OK** button to save the schedule.



Schedules are stored using the Windows Task Scheduler.

You can have as many scheduled tasks that you want. You view and modify all of the scheduled tasks bring up the **Currently Scheduled Tasks** window by selecting **Schedule** in the left hand menu.
From the **Currently Scheduled Tasks** window you can edit a task by pressing the **Edit Task Schedule** button, remove a task by pressing the **Remove Task** button, run a task immediately by pressing the **Run Task Now** button, or open the task in a new session with the **Open Scheduled Task** in New Session button.

A scheduled task can run when there is no interactive session with a logged in user. It will run in the background. When the scheduled task is complete it will create a **Task Output Session**. These task output sessions are viewed from the Schedule window by selecting one and pressing the **Open Task Output Session** button. They are saved until they are deleted with the **Remove Selected Task Output Session button**.

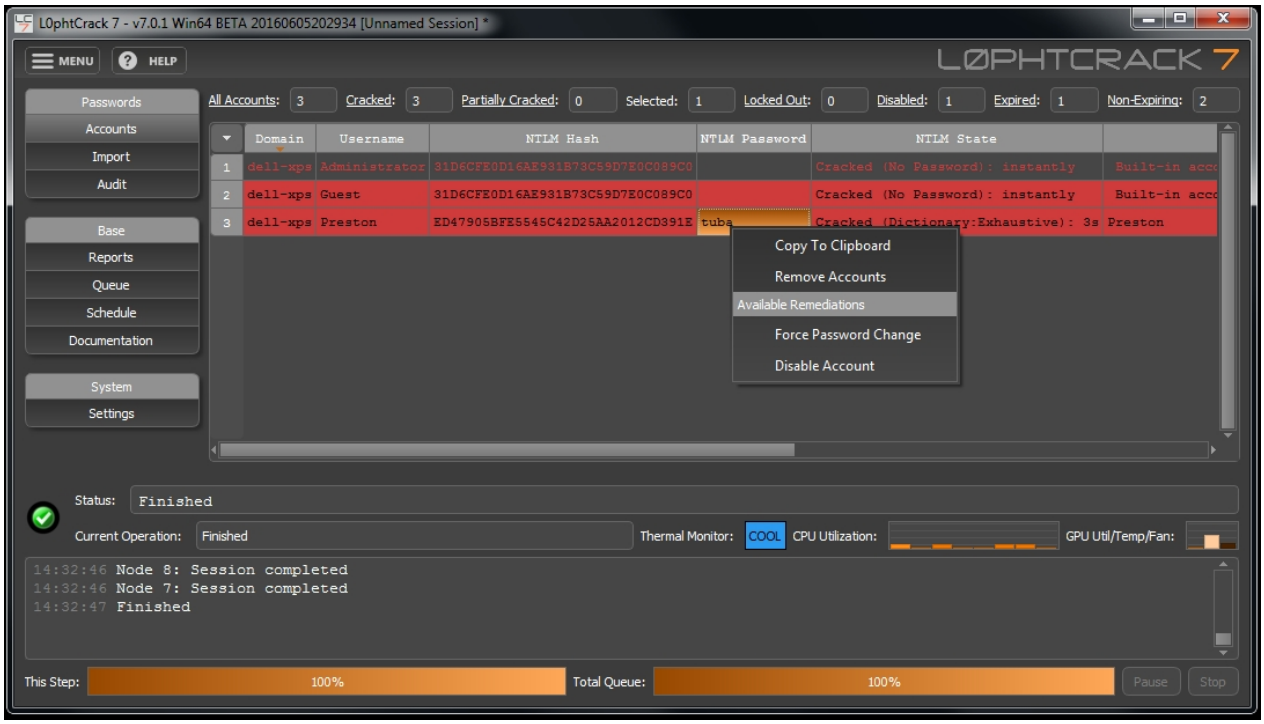


Remediating Poor Passwords

Once you have run a password audit and discovered weak passwords you are likely going to want to remediate them. You can right click on an acount in the main window and if there are available remediations they will be displayed. Remediations are available if you imported the passwords from the local machine or a remote machine. They are not available if you imported from a file because L0phtCrack doesn't have the credentials and the associated machine to connect to in order to perfrom the remediation.

To remediate, right click on the account you want to remediate and select **Disable Account** or **Force Password Change** from the **Available Remediations** pop up menu. Multiple accounts can be selected by holding down the shift or control keys while clicking. It is convenient to sort all the cracked passwords, select them, and choose a remediation option. **Please be careful not to disable the Administrator account!** If you do, you won't be able to get back into it to enable it again.

Due to the sensitive nature of remediation, it may only be performed interactively, and not scheduled.



Reporting

L0phtCrack 7 reports include:

- Export Accounts Table

Upon completion of the audit, results can be exported by selecting **Reports** from the left hand menu. From the **Reports** window choose the **File Format**:

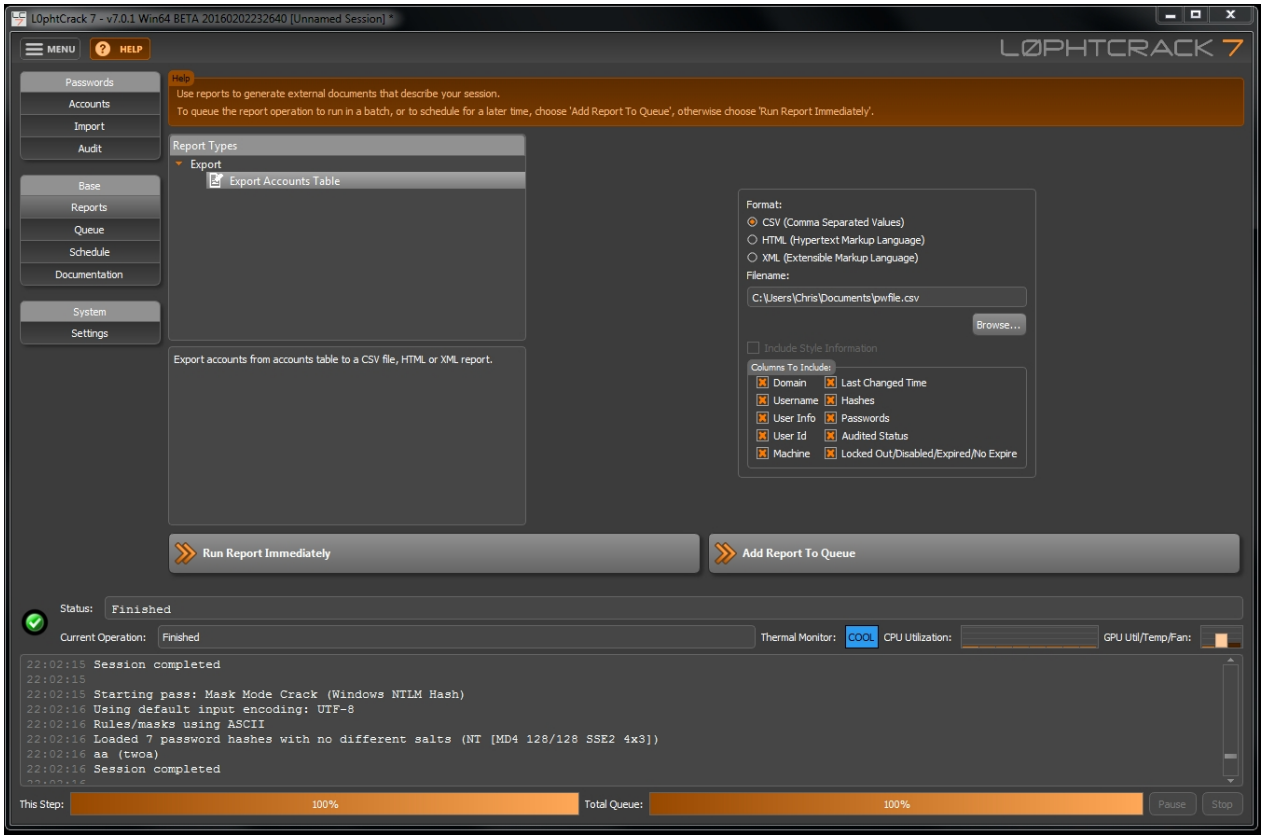
- CSV (Comma Separated Values)
- HTML (Hypertext Markup Language)
- XML (Extensible Markup Language)

Select a **Filename** to save the report to.

Select one or more **Columns** to include in the report:

- Domain
- Username
- User Info
- User ID
- Machine
- Machine
- Last Changed Time
- Hashes
- Passwords
- Audited Status
- Locked Out/Disabled/Expired/No Expire

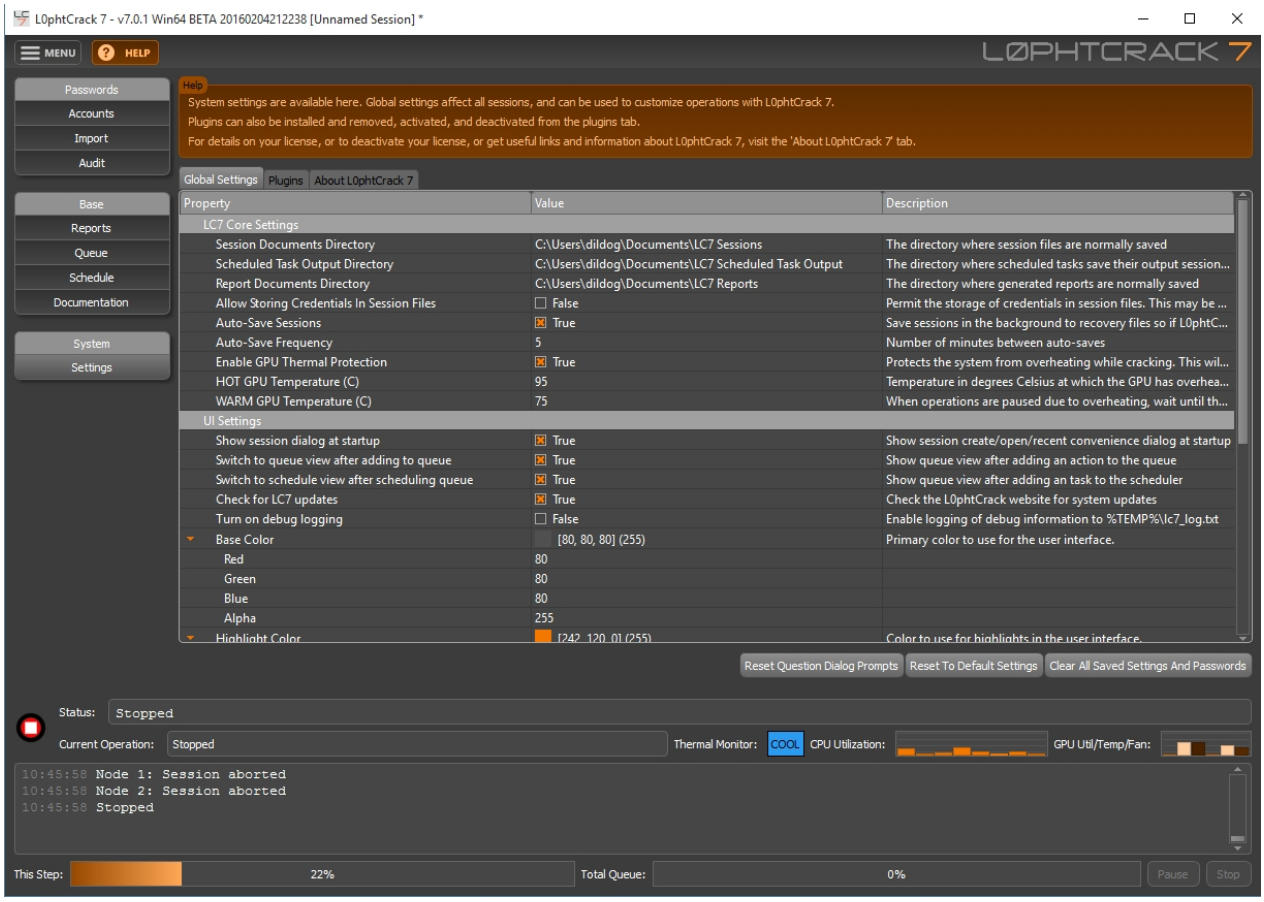
You can run the report immediately by selecting **Run Report Immediately** or add it to the queue by selecting **Add Report to Queue**.



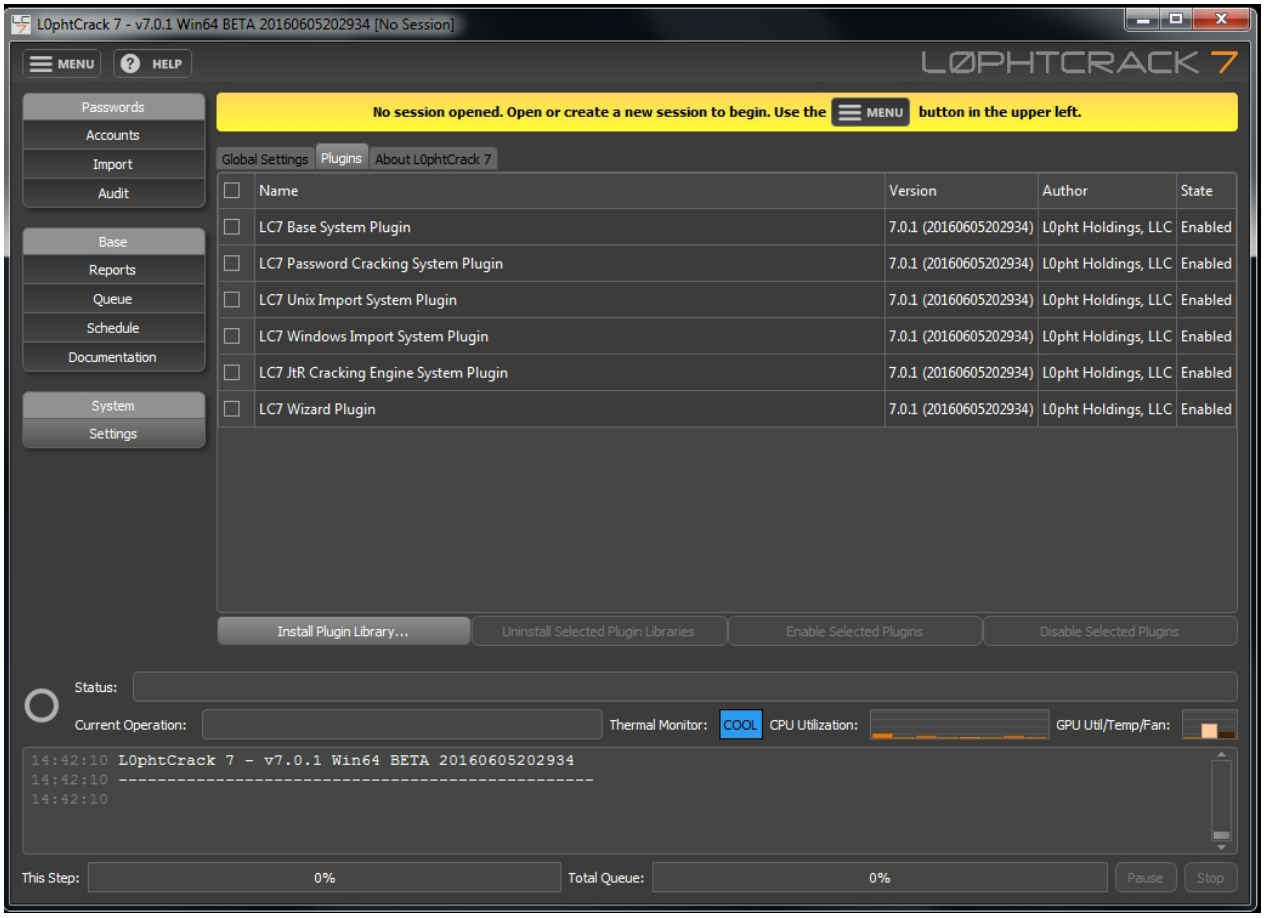
Settings

Select **Settings** from the left side side to display the **Settings**. There are three tabs: **Global Settings**, **Plugins**, and **About L0phtCrack 7**

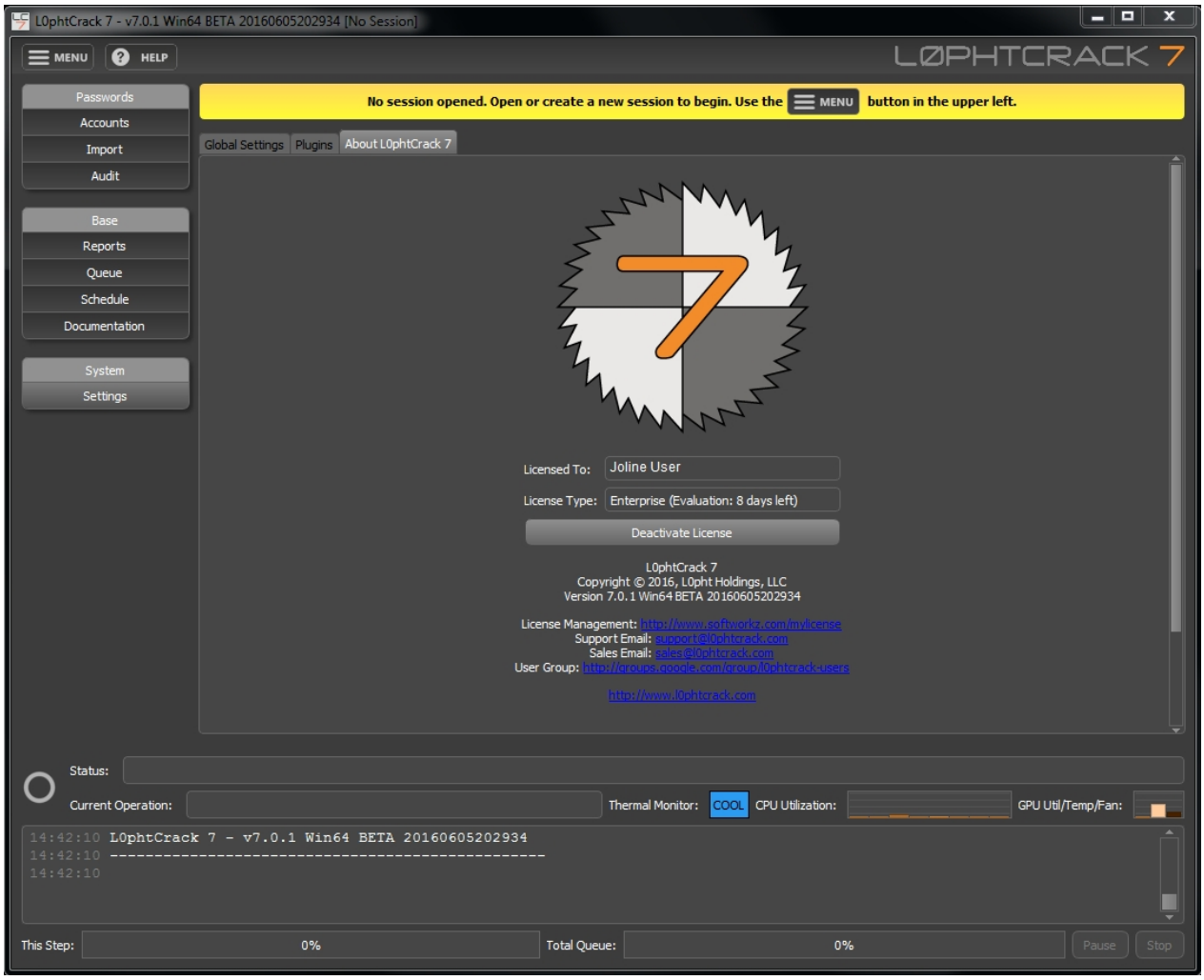
The **Global Settings** allow you so set options such as default directories, customize the UI, and enable or disable features of the included JtR Cracking engine.



The **Plugin** tab allows you to **Install**, **Uninstall**, **Enable**, or **Disable** selected plugins. L0phtCrack 7 ships with plugins to support the base system, cracking, unix importing, windows importing, the JtR cracking engine, and the wizard. In the future additional plugins will be available for importing different types of password hashes and cracking different types of password hashes.



The **About** tab displays license info: licensee, license type, and days left it is an evaluation license. The **About** tab has a **Deactivate License** button to deactivate the license on this machine. This allows the license to be installed on another machine. There is also a display of the version information and links to the license management site and L0phtCrack support.



L0phtCrack 7 Menu Reference

The following sections describes the commands available from the MENU.

New Session
L0phtCrack uses a session file to store the settings, imported data, and progress of an auditting session. There needs to be an active session before any password hash data can be imported. Select **New Session** to create a new session. Session files use the .lc7 extension which is associated with the L0phtCrack program. The Password Auditting Wizard will also create a new session. After creating a new session you will want to import password hashes
and then configure an audit.
Open Session...
Open Session will display a file open dialog box where you can select and open a previously saved session file.

Recent Sessions
Recent Sessions will display a cascaded menu where you can select recently used session files for opening.

Recover Autosaved Session...
Auditting sessions can span many days which increases the likelihood that your computer will crash, hang or reboot during an auditting session. By default L0phtCrack autosaves a temporary session file every 5 minutes. If your session has abnormally ended use **Recover Autosaved Session...** to display a dialog box which lets you select the last autosaved temporary session file.

Save Session
Save Session will save the current session to the current session file.

Save Session As...
To save your session to a new file select **Save Session As...** to specify the session file name. You can also overwrite a previously saved session file.

Close Session
If you want to close your session and have no session open select **Close Session**. If the session isn't saved you will be prompted to save the session to a session file.

Generate Remote Agent
Typical L0phtCrack usage will not require the generation of a remote agent. L0phtCrack will be able to automatically install a remote agent as part of the remote Windows import process. However some configurations may require the manual installation of the remote agent. If this is necessary Select **Generate Remote Agent** and follow the instructions for manually installing a remote agent.

Perform Calibration
L0phtCrack can select between different processors and processor instructions available to optimize the speed of the password auditting process. L0phtcrack can run a calibration to detect the performance of the available options. The first time L0phtCrack is run you are prompted to run a calibration. This is highly recommended. If you have never run calibration or you wish to recalibrate due to hardware or driver changes you can select **Perform Calibration**.

Password Auditing Wizard
To simplify the process of password auditing you can use the **Password Auditing Wizard**. This wizard will walk you through the process of importing password hashes and selecting audit techniques. See the Wizard Overiew.

Fullscreen
Select **Fullscreen** to put L0phtCrack in fullscreen mode or to exit fullscreen mod. A checkmark will display next to the Fullscreen menu item when L0phtCrack is in fullscreen mode.

Minimize To System Tray
If you want to remove L0phtCrack from the list of running applications so it doesn't show up in the taskbar or when you alt-tab you can select **Minimize To System Tray**. An LC7 system tray icon will appear. L0phtCrack will continue running. Click on the LC7 system tray icon to restore L0phtCrack as a running application.

Check For Updates
By default L0phtCrack will check for updates everytime it is run. This can be disabled from the Settings screen. You can manually check for updates at any time by selecting **Check For Updates**. If an update is available it will be displayed and you will be able to choose to install it.

Quit
Select **Quit** to exit L0phtCrack.

Password Security in Your Organization

There are several things you can do to improve password security in your organization, in no particular order:

- Use a very strong Administrator or root password and do not share it or reuse it on any other account or system.
- Long passwords with greater than 12 characters are very strong if they are not dictionary words and contain symbol character, numbers, and both capital and lowercase letters.
- Do not reuse passwords on multiple systems with the same account name. If one system is compromized the password can be cracked and tried on other systems with the same account name.
- Establish a password policy for organization members.
- Enable strong password enforcement on Windows. On the administration console locate Local Security Policy. Select Account Policy, then Password policy, then enable Passwords must meet complexity requirements.
- Perform regular audits using L0phtCrack 7 to test the passwords in use. Even with Windows strong password enforcement users may be able to create weak passwords such as Password1.
- Restrict permissions on your Windows SAM and Unix password files.
- Restrict physical access to machines (particularly domain controllers).

Appendix

Technical Support

L0phtCrack 7 users who have purchased maintenance receive free technical support by email. Technical support is included for first year.
To receive technical support, you can open a support ticket. See www.l0phtcrack.com for details or email support@l0phtcrack.com.

To file a bug report, email support@l0phtcrack.com.

Direct technical support is not provided for those without a maintenance contract, or non-registered or trial users. A public Google Group exists for community support of L0phtCrack 7 and for general Q&A: https://groups.google.com/forum/#!forum/l0phtcrack-users

System Requirements

Operating Systems:

Windows 10, Server 2012 R2, Server 2012, 8.1, 8, 7, Server 2008 R2, Server 2008, Vista, Server 2003 (SP3 x86, SP1 x64), XP (SP3 x86, SP1 x64)

CPU Requirements:

1 GHz CPU

Optional GPU:

AMD or NVIDIA GPU for OpenCL or CUDA support

Account Requirements:

Account with Administrator Privileges

When installing L0phtCrack 7, you must be logged into an account that has administrator privileges. L0phtCrack 7 runs on Microsoft Windows operating systems. System requirements are the same as the minimum requirements for the operating system.

Supported Password Environments and Hash Types:

- Windows (LM and NTLM)
- Linux Centos 6+, Debian 7+, Fedora 15+, OpenSuse 13.2+, Ubuntu 12.04+, and possibly others (DES, MD5, Blowfish, SHA-256, SHA-512)
- FreeBSD, OpenBSD (DES, MD5, Blowfish, SHA-256, SHA-512)
- Solaris 10, 11 (DES, MD5, Blowfish, SHA-256, SHA-512)
- AIX 7+ (MD5, SHA-1, SHA-256, SHA-512, Blowfish)

Word List Format

You may use a word list of your own for dictionary cracks. To do so, your word list must consist of a single word on each line of a simple text-based file, as in the following example:

apple
dog
cat
peach

The word list is not case sensitive, and will recognize both NT and Unix formatted text files.

FAQ

Password Quality Category

Q. Is there a setting for me to change the Minimum Password Length for reporting purposes?
A. No. One option would be to export the report and import it into Excel.

Q. Is there a way to segregate specific accounts for the utilization of Brute Force Attacks. The situation is when I want to target specific accounts or perform brute force on those accounts that did not crack using the dictionary or user information?
A. Yes. You can limit accounts by deleting those accounts you do not want to crack. Delete accounts by highlighting and hitting the Delete key.

Active Directory Support

How one may connect to Active Directory, various usage scenarios, and requirements

Q. Describe how to use L0phtCrack 7 to determine password complexity compliance with Active Directory? Is it as simple as running L0phtCrack 7 on a workstation and pointing to a domain controller as the "Remote System" or is there more to it than that? I understand that you would need Domain Administrator rights to perform the analysis.
A. It is as simple as importing from a remote machine and selecting Active Directory as the machine. You need Administrator privileges on the machine. Typically Domain Administrators have this privilege.

Q. What exactly do I need in order to obtain the password hashes from a remote Active Directory domain controller? I know that local admin privileges will suffice, but I need to know specifically what I need in order for L0phtCrack 7 to extract the hashes.
A. You need the debug privilege.

Q. I have been trying to use the L0phtCrack 7 product to decrypt passwords on my server, I am using the product with active directory and every time I use the wizard an error message comes back saying no encrypted passwords were imported. The L0phtCrack 7 wizard cannot continue please try another password retrieval method to continue. What do I need to do for the product to work?
A. You need Administrator privileges on the Active Directory machine. The machine also needs to be able to be remotely administered if you are running L0phtCrack 7 on another machines and importing the password hashes remotely.

Remote Scans

Q. When you use L0phtCrack 7 to retrieve password hashes from remote machines is the data encrypted whilst being transferred?
A. Yes the data is encrypted whilst being transferred.

Selected Account Audit

Q. Is there a method by which I can either restrict, or selective choose which accounts are audited?
A. Yes, LC will let you delete accounts that you do not want to audit.

Password Recovery

Q. Why do I see a blank password field after the completion of the audit?
A. This means that the password was not cracked by L0phtCrack 7. This is typically a strong password depending on your cracking settings.

Resources

This section lists tools and information that may help in your password auditing efforts. As always, exercise the appropriate diligence in evaluating and using these resources.

fgdump (http://foofus.net/goons/fizzgig/fgdump)

fgdump runs like pwdump to allow remote access to the password database on SYSKEY protected systems, and is available for free from fizzgig. Its output is a similar format to the .lc format used by L0phtCrack 2.5. L0phtCrack 7 can import files that fgdump outputs as they are compatible with pwdump. fgdump plays better with anti-virus systems and is recommended over pwdump.

pwdump (https://en.wikipedia.org/wiki/Pwdump)

pwdump is the name of various Windows programs that output the LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM). In order to work, it must be run under an Administrator account, or be able to access an Administrator account on the computer where the hashes are to be dumped. Pwdump could be said to compromise security because it could allow a malicious administrator to access user's passwords. Most of these programs are open-source.

L0phtCrack 7 can import files that pwdump outputs.

Password Reset Utility

You must have access to at least one administrator account on a Windows machine in order to obtain password hashes from that machine, whether you use fgdump, or L0phtCrack 7's own Import From Local Machine feature. The only other way to access the machine might be through a password reset utility such as the following: http://pogostick.net/~pnh/ntpasswd/.

Source Code

The core of L0phtCrack 7's engine is based on the John The Ripper project:

- John The Ripper 'Jumbo' project: https://github.com/magnumripper/JohnTheRipper
- The JTRDLL fork of John The Ripper used in L0phtCrack 7: https://github.com/L0phtCrack/jtrdll

The original source code L0phtCrack 1.5 is available in an open source version for research purposes from http://insecure.org/stf/lc15src.tgz

Included Software

L0phtCrack 7 incorporates the following third-party software, the licenses for which are reproduced here for compliance:

OpenSSL: https://www.openssl.org

```
/* ====================================================================
 * Copyright (c) 1998-2016 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
```

```
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

ADL SDK 8: Copyright (c) Advanced Micro Devices, Inc.

Chilkat Libraries: http://www.chilkatsoft.com/

Chilkat Software License

PLEASE READ THIS AGREEMENT BEFORE OPENING THIS SOFTWARE PACKAGE. IF YOU OPEN THIS PACKAGE

(1) DEFINITION OF TERMS

"Documentation": any explanatory written or on-line material including, but not limited t

"Licensee": shall refer to the individual licensee, whether as an individual programmer,

"Software": All material in this distribution including, but not limited to, one or more

"Licensed Software": the Software for which Licensee has paid the applicable license fee

"Software Application Programming Interface ("API")": the set of access methods, whether

"End-User Software Product": an application developed by Licensee intended for execution

The Licensed Software contains certain runtime libraries and files intended for duplicati

SPECIAL LIMITED TERM EVALUATION LICENSE

If Licensee has been provided with a copy of the Software for evaluation purposes, Chilka

(2) GENERAL

The Software is owned by Chilkat Software, Inc. ("Chilkat") and is protected by U.S. copy

(3) LICENSE GRANTS

(a) Per-developer license. Subject to the terms and conditions of this Agreement , Chilka

(b) Site-wide license. If you have purchased a site-wide license, the following rights ap

Licensee may also:

(i) Make one backup copy of the Licensed Software solely for archival and disaster-recove

(ii)Reproduce and distribute the Redistributable Components directly or indirectly for ar

(iii) The license rights granted under this Agreement do not apply to development and dis

Licensee has no rights to use the Licensed Software beyond those specifically granted in

(4) LICENSE RESTRICTIONS

EXPORT CONTROLS: If the Software is for use outside the United States of America, License

Notwithstanding any provisions in this Agreement to the contrary, Licensee may not distri

In addition, Licensee may not decompile, disassemble, or reverse engineer any object code

(5) TITLE

Licensee acknowledges and agrees that all right, title and interest in and to the Softwar

(6) NON-TRANSFERABILITY

Except for Licensees rights to distribute the Redistributable Components, Licensee may no

(7) LIMITED WARRANTIES

Chilkat warrants to Licensee that the Licensed Software will substantially perform the fu

EXCEPT AS EXPRESSLY SET FORTH ABOVE, CHILKAT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, EX

(8) LIMITATION OF LIABILITY

IN IN NO EVENT SHALL CHILKAT BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCID

(9) TERMINATION

Chilkat reserves the right, at its sole discretion, to terminate this Agreement upon writ

(10) MISCELLANEOUS

Applicable Law and Jurisdiction. This Agreement will be governed by and construed in acco

Limitation of Actions. No action, regardless of form, may be brought by either party more

Invalidity and Waiver. Should any provision of this Agreement be held by a court of law t

U.S. Government Restricted Rights. The Licensed Software is provided with Restricted Righ

LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS IT AND AGREES TO BE BO

CrashRpt: http://crashrpt.sourceforge.net/

Copyright (c) 2003, The CrashRpt Project Authors.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name of the author nor the names of its contributors
  may be used to endorse or promote products derived from this software without
  specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES

OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

John The Ripper Community-Enhanced Jumbo Edition: https://github.com/magnumripper/JohnTheRipper

Core used with license from Alexander Peslyak. GPL-Compliant code available at: https://github.com/L0phtCrack/jtrdll

John the Ripper copyright and license.

John the Ripper password cracker,
Copyright (c) 1996-2013 by Solar Designer.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

As a special exception to the GNU General Public License terms, permission is hereby granted to link the code of this program, with or without modification, with any version of the OpenSSL library and/or any version of unRAR, and to distribute such linked combinations. You must obey the GNU GPL in all respects for all of the code used other than OpenSSL and unRAR. If you modify this program, you may extend this exception to your version of the program, but you are not obligated to do so. (In other words, you may release your derived work under pure GNU GPL version 2 or later as published by the FSF.)

(This exception from the GNU GPL is not required for the core tree of John the Ripper, but arguably it is required for -jumbo.)

Relaxed terms for certain components.

In addition or alternatively to the license above, many components are available to you under more relaxed terms (most commonly under cut-down BSD license) as specified in the corresponding source files.

Furthermore, as the copyright holder for the bcrypt (Blowfish-based password hashing) implementation found in John the Ripper, I have placed a derived version of this implementation in the public domain. This derived version may be obtained at:

http://www.openwall.com/crypt/

The intent is to provide modern password hashing for your servers and
your software (where the GPL restrictions could be a problem).

      Commercial licensing.

Commercial licenses (non-GPL) are available upon request.

      Copyright holder contact information.

For the core John the Ripper tree:

Alexander Peslyak aka Solar Designer <solar at openwall.com>

(There are additional copyright holders for "community enhanced" -jumbo
versions of John the Ripper.)

Owl

NVIDIA NVAPI

NVIDIA Corporation

Software License Agreement

NVAPI SDK

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING

Do not use or load the software tools and any associated materials provided by NVIDIA on
“Licensee,” “You” and/or “Your” shall mean, collectively and individually, the company or
“Derivative Works” shall mean derivatives of the Software created by You or a third party
“Intellectual Property Rights” shall mean all proprietary rights, including all patents,

SECTION 1 - GRANT OF LICENSE.
NVIDIA agrees to provide the Software and any associated materials pursuant to the terms
(a) install, deploy, use, have used execute, reproduce, display, perform, run, modify the
in part or whole, into Your software applications that execute on or use NVIDIA hardware
(b) to transfer, distribute and sublicense Your Derivative Works, in whole or in part, ar
If You are not the final manufacturer or vendor of a computer system or software program
Except as expressly stated in this Agreement, no license or right is granted to You direc

SECTION 2 - CONFIDENTIALITY. If You receive the NVAPI SDK (any version), any exchange of
If You wish to have a third party consultant or subcontractor ("Contractor") perform work

SECTION 3 - OWNERSHIP OF SOFTWARE AND INTELLECTUAL PROPERTY RIGHTS.
All rights, title and interest to all copies of the Software remain with NVIDIA, subsidia
All rights, title and interest in the Derivative Works of the Software remain with You su
You have no obligation to give NVIDIA any suggestions, comments or other feedback (“Feedb

SECTION 4 - NO WARRANTIES.
THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INC

SECTION 5 - LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO THE MISUSE OF THE OTHER PARTY
FOREGOING, NVIDIA’S AGGREGATE LIABILITY ARISING OUT OF THIS AGREEMENT SHALL NOT EXCEED ON

SECTION 6 - TERM.

This Agreement and the licenses granted hereunder shall be effective as of the date You d

SECTION 7 - TERMINATION.
NVIDIA may terminate this Agreement at any time if You violate its terms. Upon terminatio

SECTION 8 – MISCELLANEOUS.
SECTION 8.1 - SURVIVAL.
Those provisions in this Agreement, which by their nature need to survive the termination
SECTION 8.3 - AMENDMENT.
The Agreement shall not be modified except by a written agreement that names this Agreeme
SECTION 8.4 – NO WAIVER.
No failure or delay on the part of either party in the exercise of any right, power or re
thereof, nor shall any single or partial exercise of any right, power or remedy preclude
SECTION 8.5 – NO ASSIGNMENT.
This Agreement and Licensee's rights and obligations herein, may not be assigned, subcont
SECTION 8.6 - GOVERNMENT RESTRICTED RIGHTS.
The parties acknowledge that the Software is subject to U.S. export control laws and regu
The Software has been developed entirely at private expense and is commercial computer so
SECTION 8.7 – INDEPENDENT CONTRACTORS.
Licensee's relationship to NVIDIA is that of an independent contractor, and neither party
SECTION 8.8 - SEVERABILITY.
If for any reason a court of competent jurisdiction finds any provision of this Agreement
SECTION 8.9 - ENTIRE AGREEMENT.
This Agreement and NDA constitute the entire agreement between the parties with respect t

QtKeychain: https://github.com/frankosterfeld/qtkeychain

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Zlib: http://www.zlib.net/

Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied
  warranty. In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it

freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes. Please read the FAQ for more information on the distribution of modified source versions.

Qt: www.qt.io

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid

distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any

warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2,

instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library

facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is

implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

  12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

  13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

  14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

  15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

  16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF

SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

ImPacket: https://github.com/CoreSecurity/impacket

We provide this software under a slightly modified version of the Apache Software License. The only changes to the document were the replacement of "Apache" with "Impacket" and "Apache Software Foundation" with "CORE Security Technologies". Feel free to compare the resulting document to the official Apache license.

The `Apache Software License' is an Open Source Initiative Approved License.

The Apache Software License, Version 1.1
Modifications by CORE Security Technologies (see above)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:
   "This product includes software developed by
    CORE Security Technologies (http://www.coresecurity.com/)."
   Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Impacket" and "CORE Security Technologies" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact oss@coresecurity.com.

5. Products derived from this software may not be called "Impacket", nor may "Impacket" appear in their name, without prior written permission of CORE Security Technologies.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Smb.py and nmb.py are based on Pysmb by Michael Teo (http://miketeo.net/projects/pysmb/), and are distributed under the following license:

This software is provided 'as-is', without any express or implied warranty. In no event will the author be held liable for any damages

```
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must
   not claim that you wrote the original software. If you use this
   software in a product, an acknowledgment in the product
   documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must
   not be misrepresented as being the original software.

3. This notice cannot be removed or altered from any source
distribution.
```

Credits

L0phtCrack 7 was developed by Christien Rioux.

Documentation and testing by Chris Wysopal and Sarah Zatko.

New topic