Content Authentication and PKI Security

1. Authentication

Authentication is the process of recognizing a user’s identity.

It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user’s information on a local operating system or within an authentication server.

The authentication process always runs at the start of the application.

1.1 Digital Signature

Provides authentication and integrity.

The digital equivalent of a handwritten signature or stamped seal.

Electronic signature.

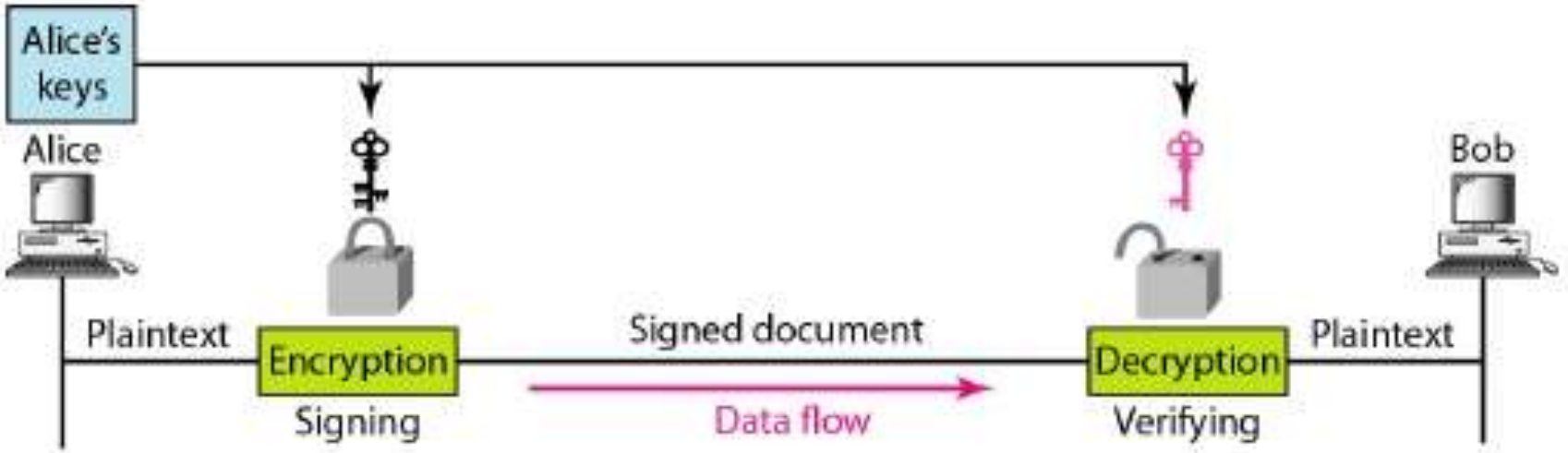
1.1 Difference

In Cryptography, Sender encrypts message using Receiver's public key and Receiver decrypts message using Receiver's private key.

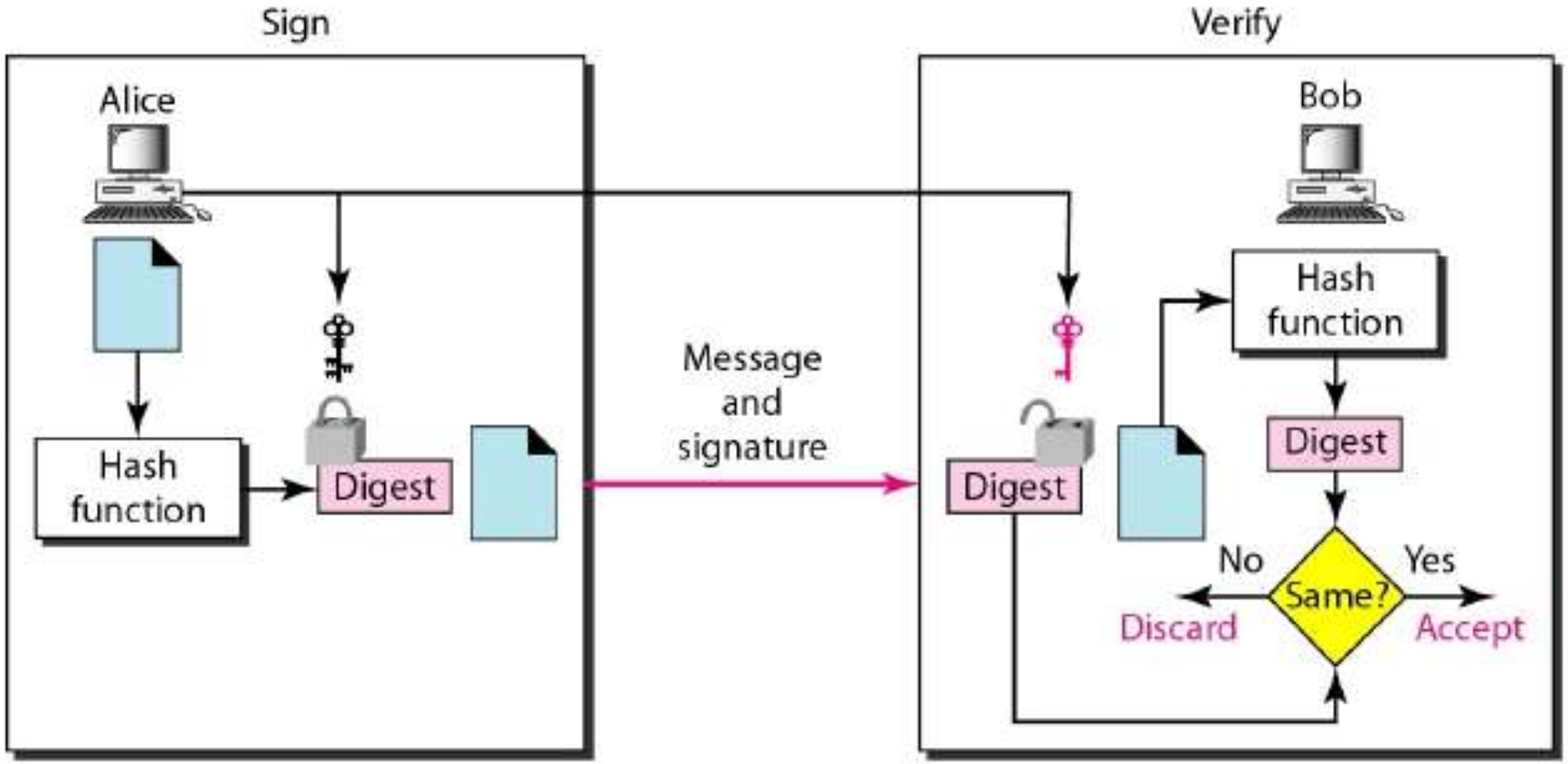
In Digital Signature , Sender encrypts message using Sender's private key and Receiver decrypts message using Sender's public key.

Thus provides authentication - whether the message came from sender's side or not.

1.2 Signing the message



1.2 Signing the digest



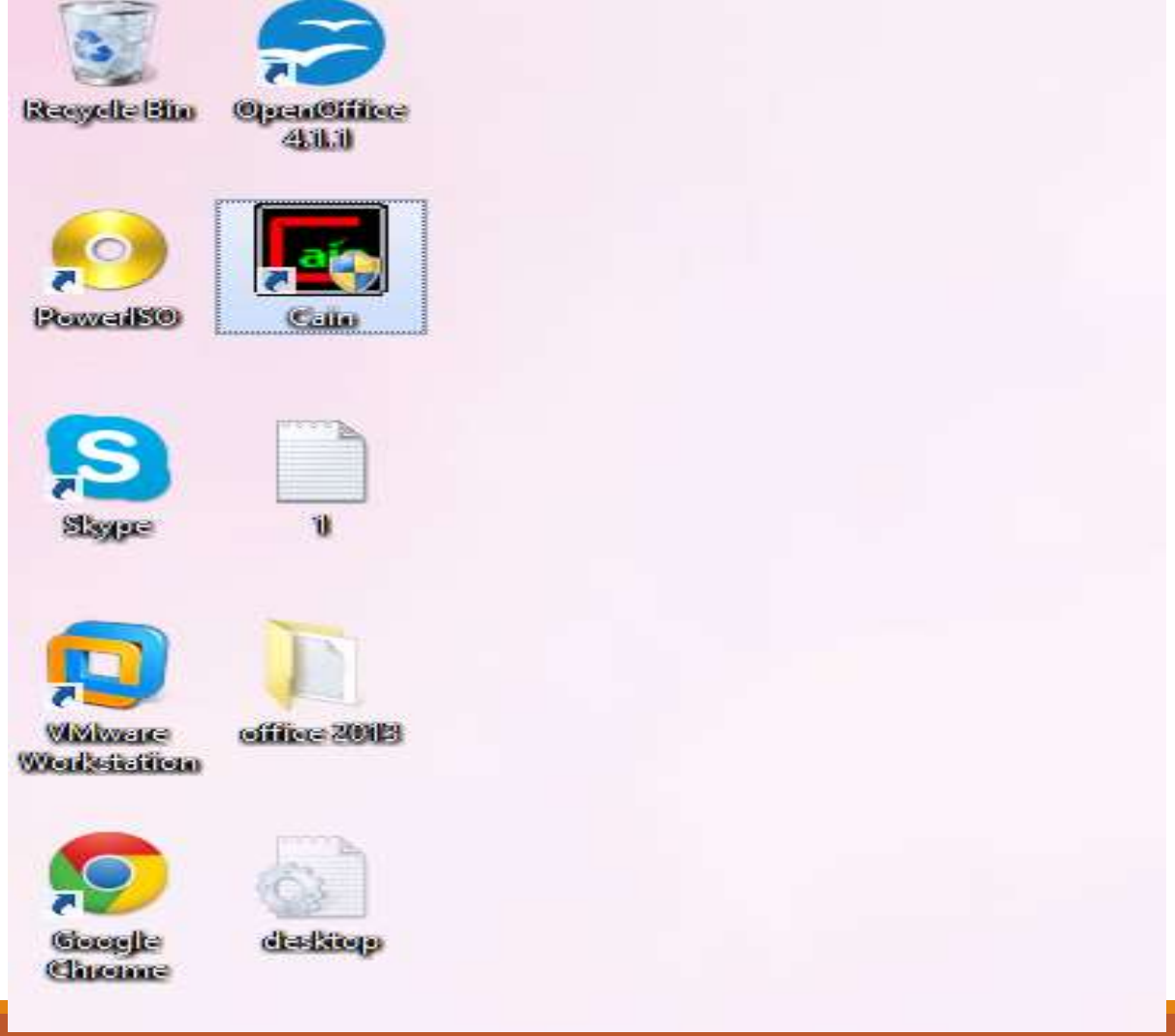
2. Practical Session to bypass authentication

1. Download and install CAIN TOOL

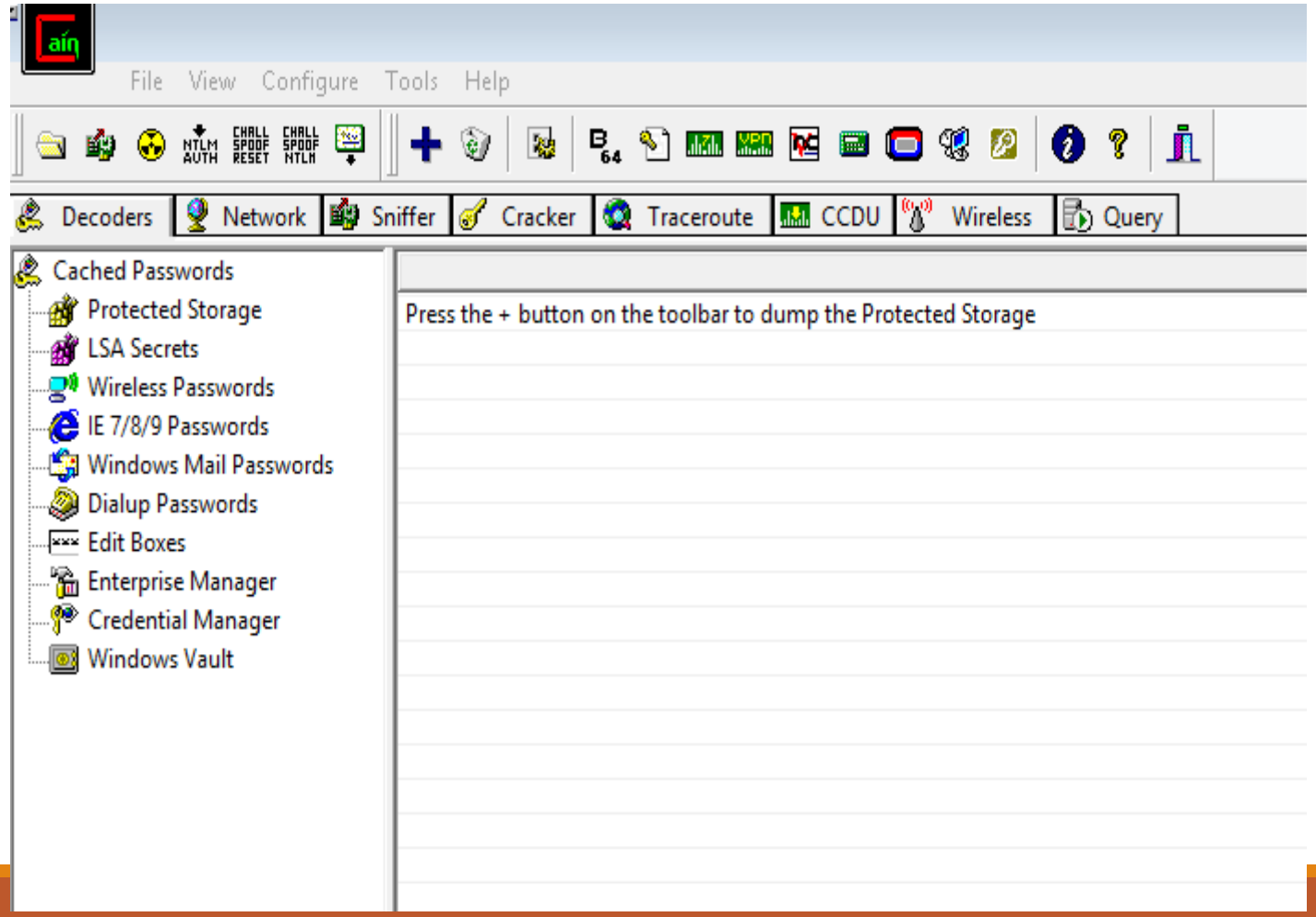
2. Check wordlist of CAIN in C:/programfiles/cain

3. Create a new account in Windows machine

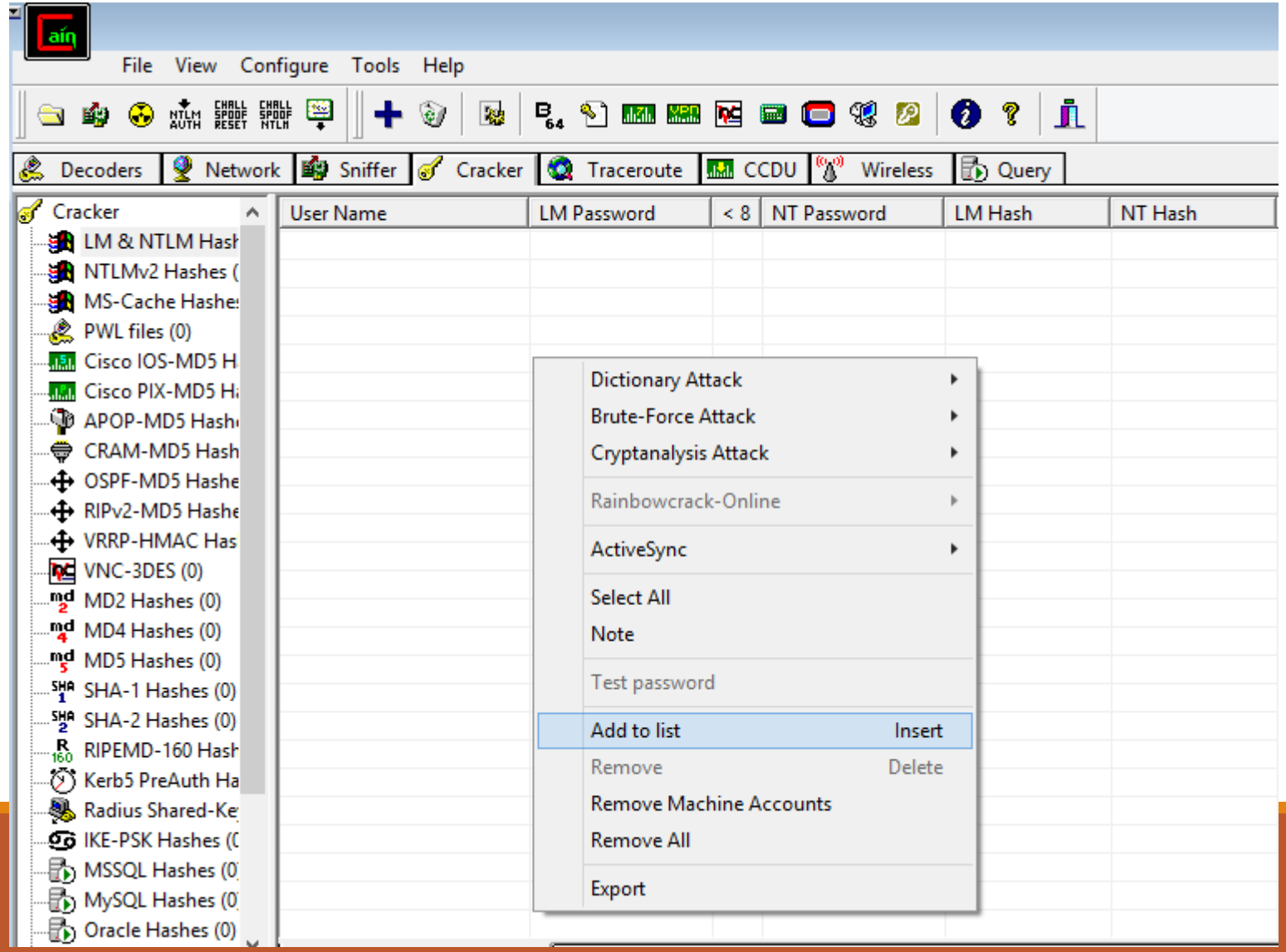
4. Set one of the password present in wordlist


Recycle Bin
OpenOffice 4.1.1
PowerISO
Cain
Skype
1
VMware Workstation
office 2013
Google Chrome
desktop

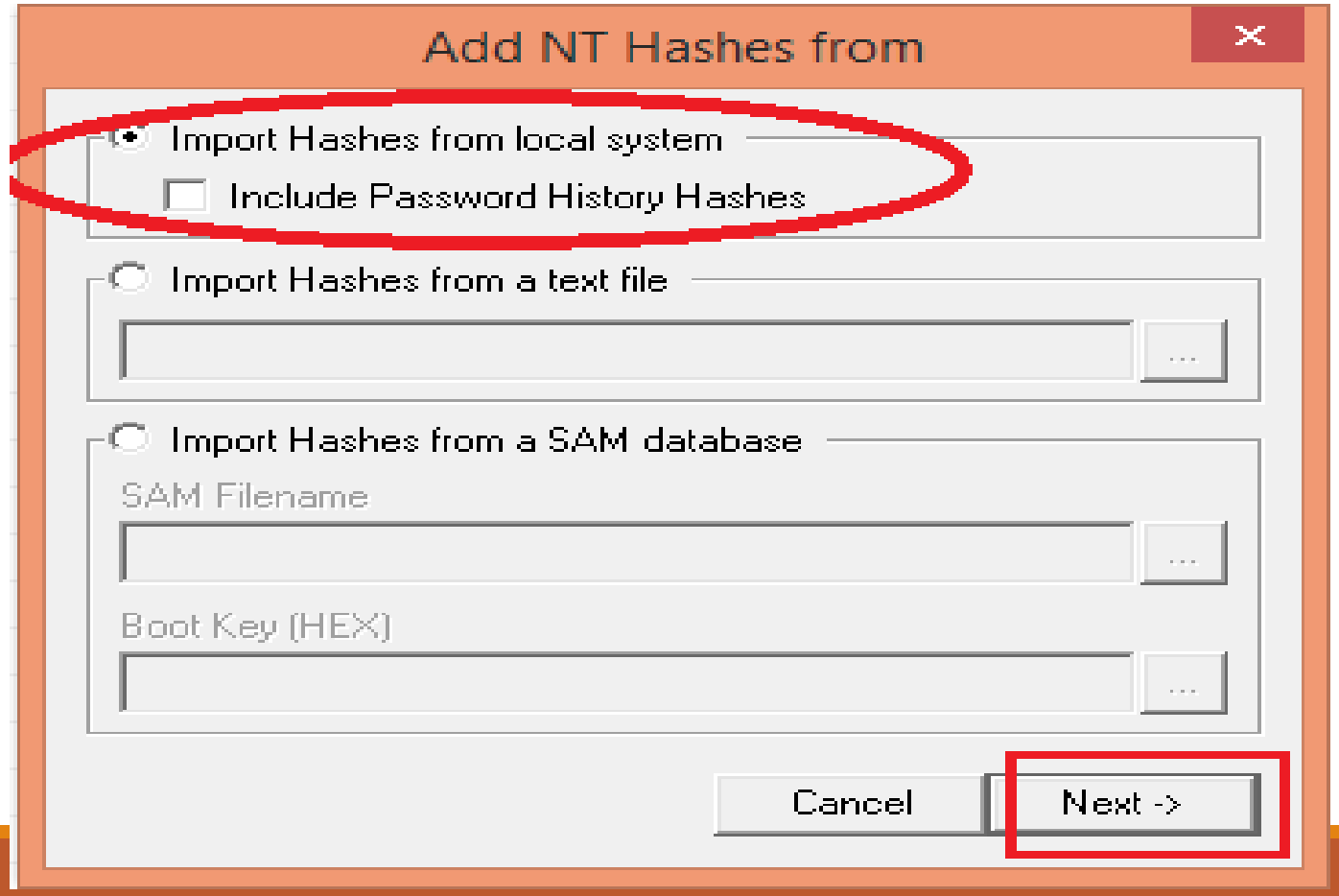
CAIN TOOL


File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Press the + button on the toolbar to dump the Protected Storage

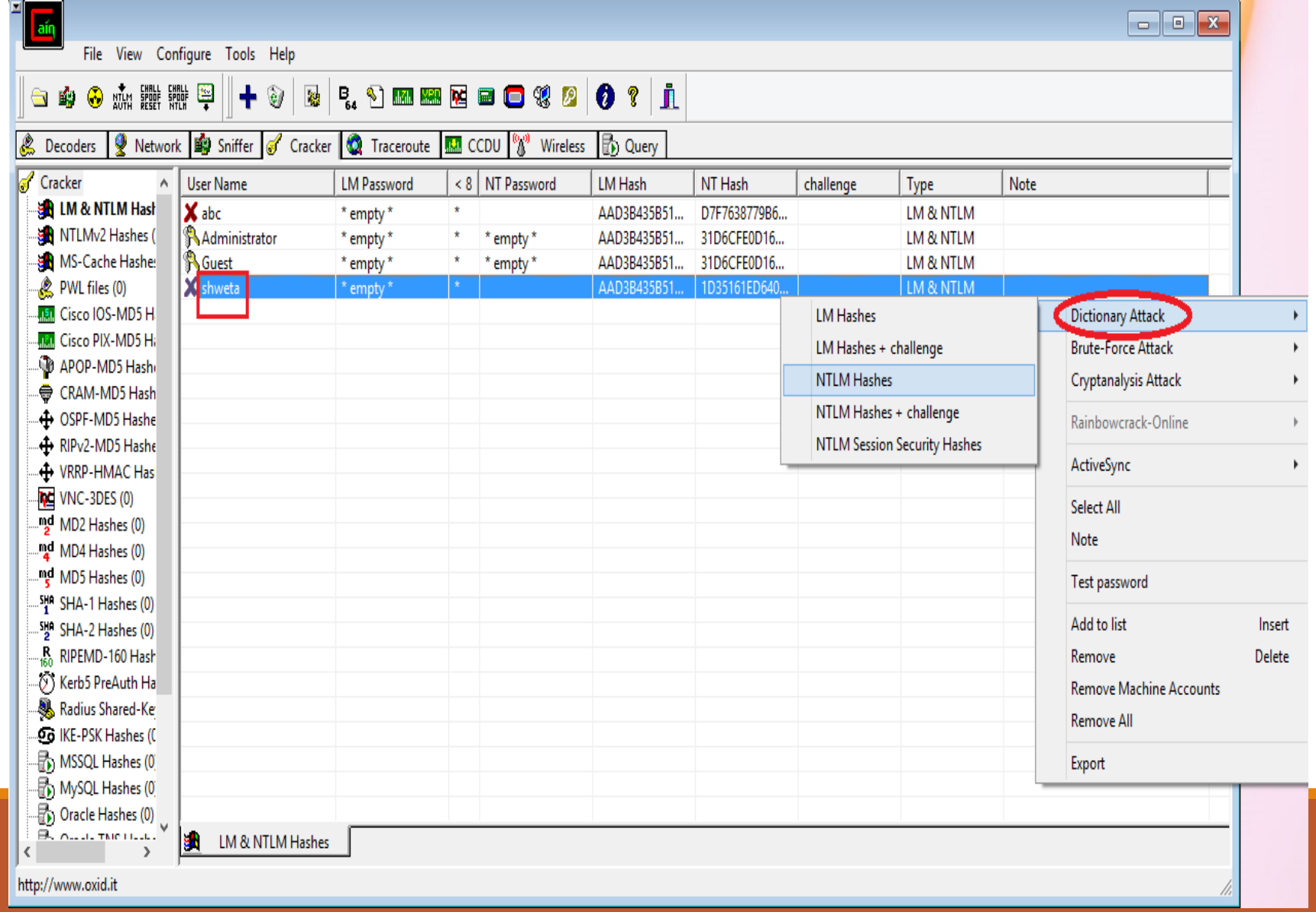
CAIN TOOL


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes (
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 Ha
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
User Name
LM Password
< 8
NT Password
LM Hash
NT Hash
Dictionary Attack
Brute-Force Attack
Cryptanalysis Attack
Rainbowcrack-Online
ActiveSync
Select All
Note
Test password
Add to list Insert
Remove Delete
Remove Machine Accounts
Remove All
Export

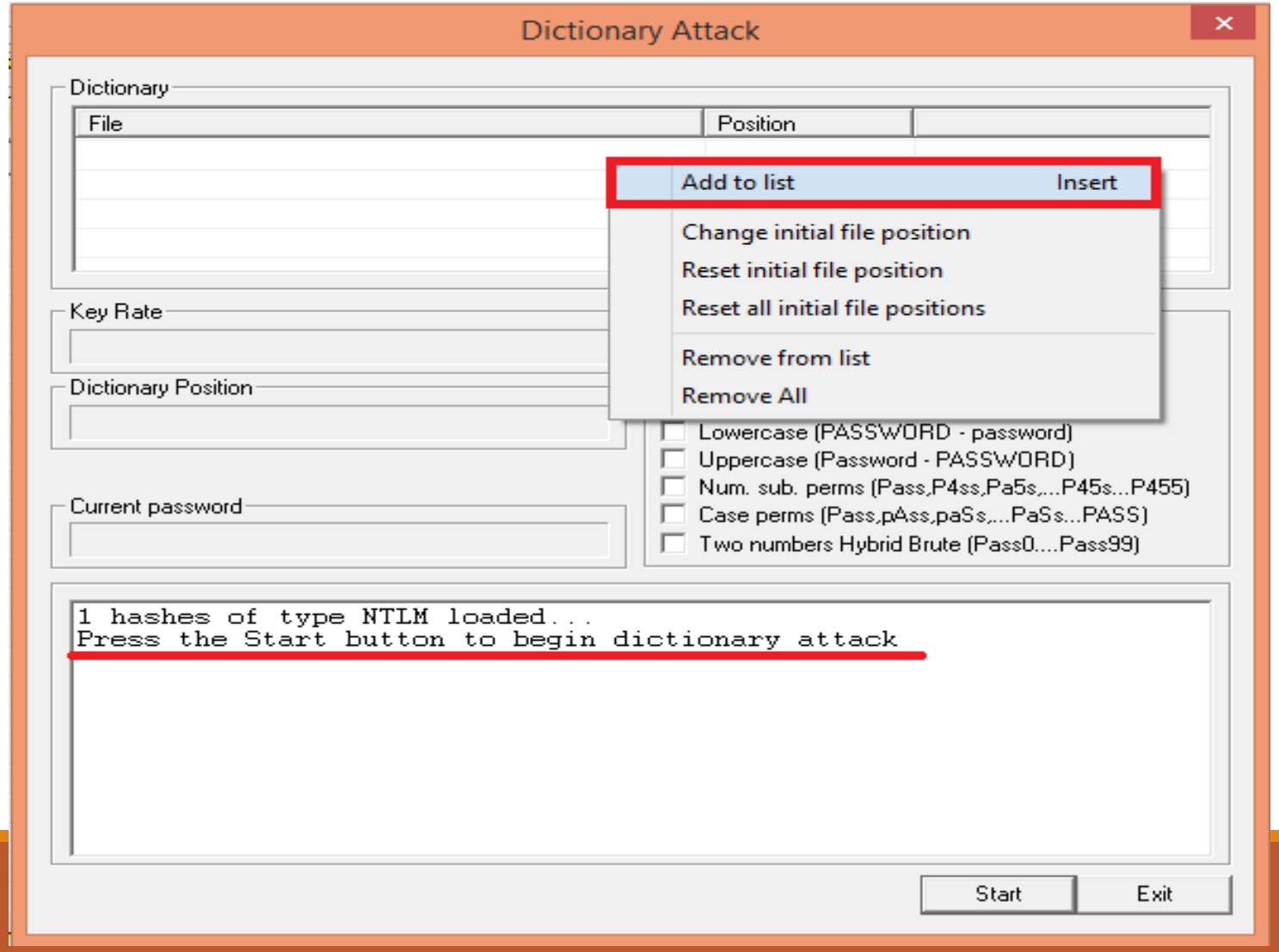
NTLM HASH



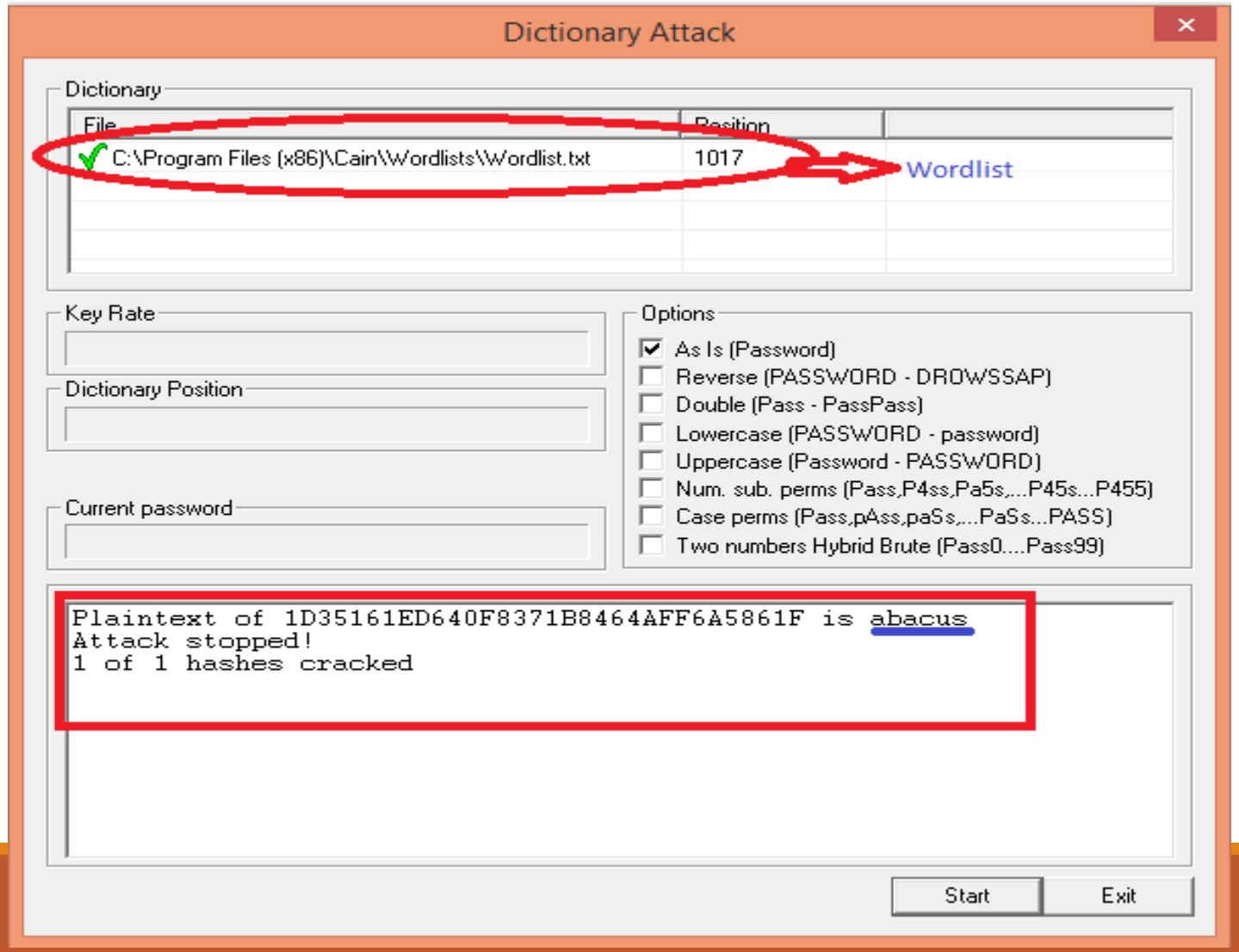
IMPORT HASH FROM SYSTEM



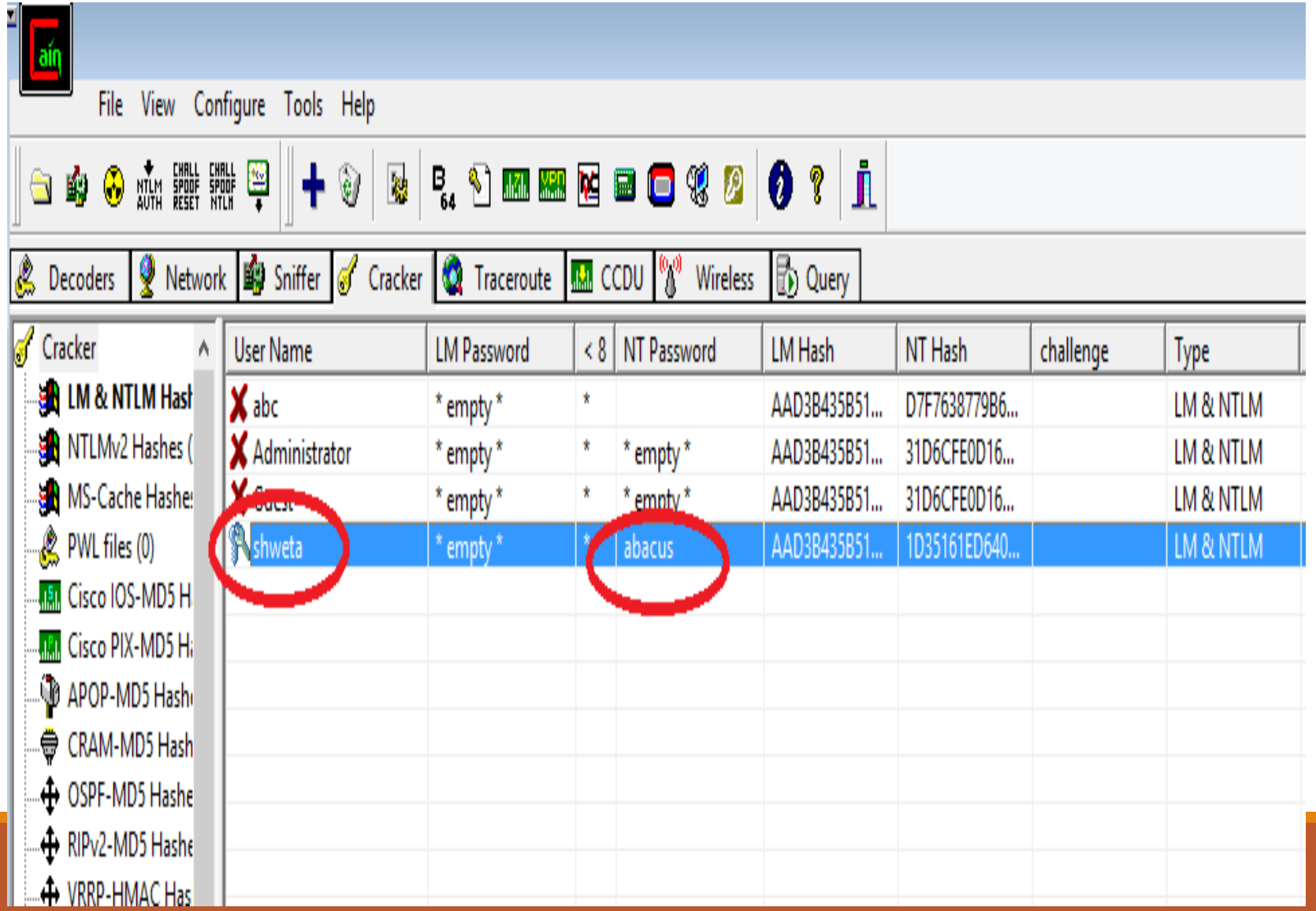
APPLY DICTIONARY ATTACK



ADD DICTIONARY TO LIST


Dictionary Attack
Dictionary
File
Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt
1017
Wordlist
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of 1D35161ED640F8371B8464AFF6A5861F is abacus
Attack stopped!
1 of 1 hashes cracked
Start
Exit

PRESS START



PASSWORD RECOVERED

3. PKI Security

Public Key Infrastructure

It uses a pair of keys to achieve security services. The key pair comprises of private key and public key.

Since the public keys are in open domain, they are likely to be abused. It is, thus, necessary to establish and maintain some kind of trusted infrastructure to manage these keys.

3. PKI Security

PKI provides assurance of public key. It provides the identification of public keys and their distribution. An anatomy of PKI comprises of the following components:

- Public Key Certificate, commonly referred to as '**digital certificate**'.
- Private Key **tokens**.
- **Certification Authority**.
- **Registration Authority**.
- **Certificate Management System**.

3.1 Digital Certificate

A certificate can be considered as the ID card issued to the person.

People use ID cards such as a driver's license, passport to prove their identity.

A digital certificate does the same basic thing in the electronic world, but with one difference.

Digital Certificates are not only issued to people but they can be issued to computers, software packages or anything else that need to prove the identity in the electronic world.

3.1 Digital Certificate

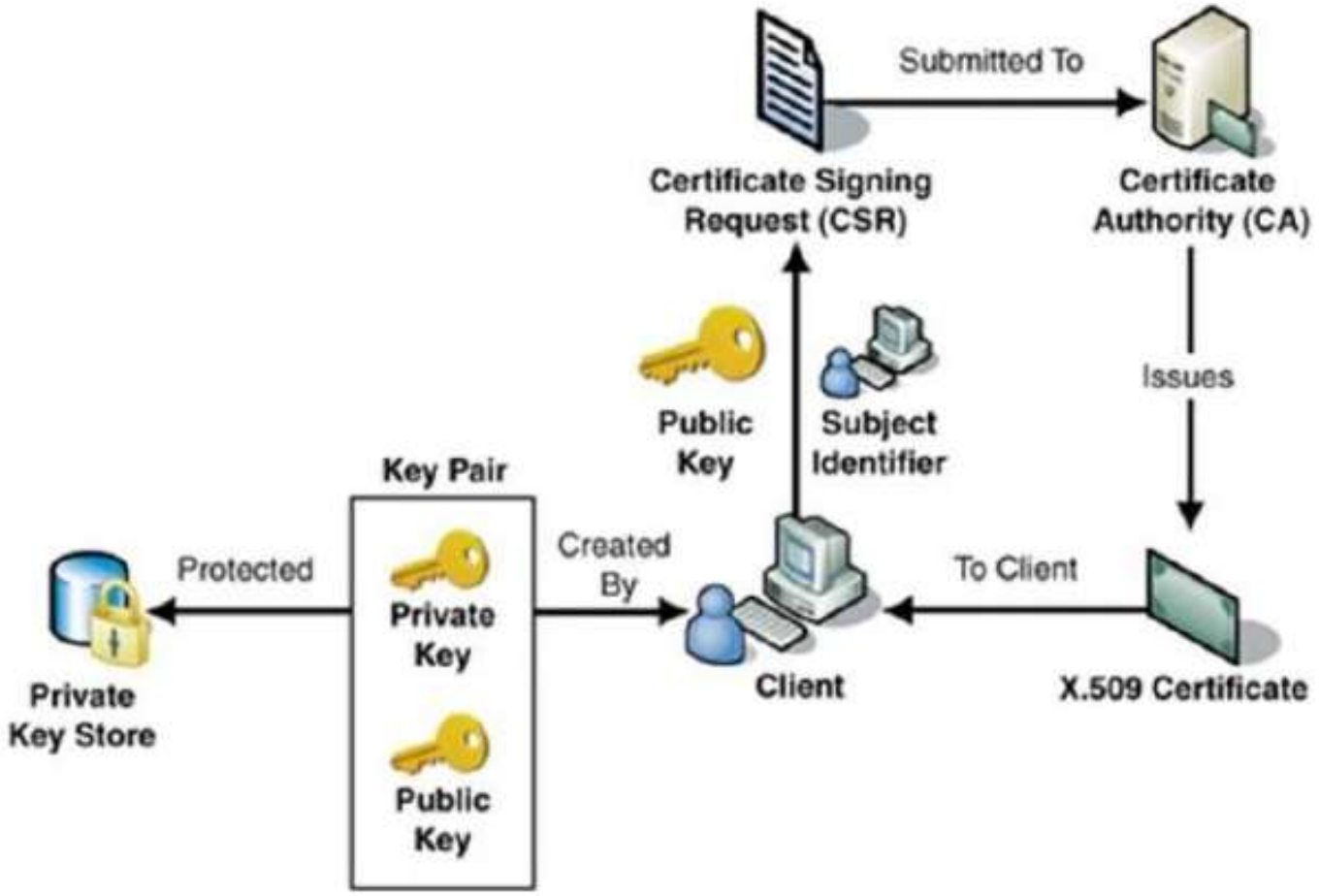
Digital certificates are based on the ITU standard X.509 which defines a standard certificate format for public key certificates and certification validation.

Hence digital certificates are sometimes also referred to as X.509 certificates.

Public key pertaining to the user client is stored in digital certificates by The **Certification Authority** (CA) along with other relevant information such as client information, expiration date, usage, issuer etc.

CA digitally signs this entire information and includes digital signature in the certificate.

3.1 Digital Certificate



3.2 Registration Authority

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity.

The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

3.3 Certificate Management System

It is the management system through which certificates are published, temporarily or permanently **suspended, renewed, or revoked**.

Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons.

A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.


thank
you