

- [AD Academic: Computer Forensics](#)
 - [AD Academic: Summation](#)
 - [Forensic Academic Partners](#)
 - [Summation Academic Partners](#)
- [Summ It Up](#)
- [News](#)
 - [Press Releases](#)
 - [Articles](#)
 - [Events](#)
- [Support](#)
 - [AD Downloads](#)
 - [AD Summation Downloads](#)
 - [Previous Releases](#)
 - [Discussion Forum](#)
 - [Contact Support](#)
 - [General Inquires / Sales](#)
 - [Technical / Customer Support](#)
 - [Knowledge Base](#)
 - [Court Reporter Information](#)
- [Company](#)
 - [Contact Us](#)
 - [General Inquires / Sales](#)
 - [Technical / Customer Support](#)
 - [Overview](#)
 - [Resellers](#)
 - [Corporate Resellers](#)
 - [Summation Resellers](#)
 - [US Federal Resellers](#)
 - [Management](#)
 - [Career Opportunities](#)
- [Technology Partners](#)
 - [FTK](#)
 - [MPE+](#)
 - [AD Lab](#)
 - [AD Enterprise](#)
 - [SilentRunner Mobile](#)
 - [Decryption](#)
 - [Triage](#)
 - [Live Response](#)
-

Decryption and Password Cracking Software

[Password Recovery Toolkit® \(PRTK®\) >](#)

[Distributed Network Attack® \(DNA®\) >](#)

[Rainbow Tables: Portable Office Rainbow Tables® \(PORT®\) >](#)

[Rainbow Tables Bundle >](#)

Password Recovery Toolkit® (PRTK®)

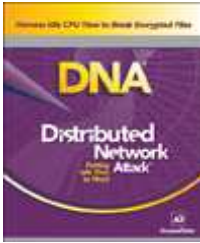


Locked out? Get back in. Password Recovery Toolkit gives you the ability to recover passwords from well-known applications. PRTK is perfect for law enforcement and corporate security professionals. If you need access to locked files or if your users have simply locked themselves out of their files, PRTK is The Key to Cracking It.

PRODUCT DETAILS:

- Enables password management.
- Analyzes files and their passwords with an optional report file.
- Recovers all types of passwords regardless of password length.
- Analyzes multiple files at one time.
- Recovers multilingual passwords.
- Prevents unauthorized use with a personal security code.
- PRTK can recover passwords from more than 80 different applications.

Distributed Network Attack® (DNA®)



DNA is a new approach to recovering password protected files. In the past, recoveries have been limited to the processing power of one machine. DNA uses the power of machines across the network or across the world to decrypt passwords. The DNA Server is installed in a central location where machines running the DNA Client can access it over the network. DNA Manager coordinates the attack, assigning small portions of the key search to machines distributed throughout the network. The DNA Client will run in the background, only taking unused processor time.

PRODUCT DETAILS:

- Easy to read Statistics and Graphs
- Add user dictionaries
- Optimization for password attacks for specific languages
- Customize user dictionaries
- Stealth client installation functionality
- Automatic Client update when updating the DNA Server
- Control what clients work on certain jobs

Supported File Formats:

- Recovers and Decrypts...
 - ARJ
 - MS Word and Excel (97 and 2000)
 - PDF 6 and below
- Recovers passwords from...
 - MS Office XP
 - PGP Disk 4, 5, 6
 - Pkzip
 - RAR up to version 2.9 of WinRAR
 - Winzip

System Requirements

All RAM requirements are based on memory available after the OS is loaded. USB is required.

PRTK™ Minimum Requirements

- Operating System: Windows® XP/2000
- Processor: Intel Pentium® III/P4/AMD Athlon™
- RAM: 2 Gb
- Hard Disk Space: 100 Mb

DNA® Supervisor Minimum Requirements

- Operating System: Windows® XP/2000
- Processor: Intel Pentium® III/P4/AMD Athlon™ RAM: 2 Gb (more if running local worker)
- Hard Disk Space: 100 Gb
- Network: 100 Mb minimum/1Gb optimal

DNA® Worker Minimum Requirements

- Operating System:
 - Windows® XP/2000
 - Macintosh OSX 10.3.9/10.4.x
 - Linux Red Hat/Fedora Core 4
 - Solaris
- Processor:
 - Intel Pentium® III/P4/AMD Athlon™
 - Power PC G4/G5
 - Sparc
- RAM: 1 Gb
- Hard Disk Space: 40 Gb

NOTE: Currently, only the English version of MS Windows platforms is being supported.

[Return to top](#)

Portable Office Rainbow Tables® (PORT®)



Rainbow Tables are pre-computed, brute-force attacks. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying

every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

A system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations using a single 3 Ghz Pentium 4 computer. With a Rainbow Table, you can decrypt 40-bit encrypted files in seconds or minutes rather than days or weeks. DNA and PRTK seamlessly integrate with Rainbow Tables.

PRODUCT DETAILS:

- 40-bit encrypted files decrypted in 5 minutes on average
- One table available: MS Word & Excel
- Completely portable, fits on your laptop
- 98.6% accuracy MS Office

[Return to top](#)

Rainbow Tables®



Rainbow Tables are pre-computed, brute-force attacks. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

A system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations using a single 3 Ghz Pentium 4 computer. With a Rainbow Table, you can decrypt 40-bit encrypted files in seconds or minutes rather than days or weeks. DNA and PRTK seamlessly integrate with Rainbow Tables.

PRODUCT DETAILS:

MS Office

MS Office 97 and 2000 derive a 40-bit encryption key from a user-supplied password. Our rainbow tables recover that 40-bit key in typically less than one minute. Once the key has been recovered, the document can be decrypted.

Adobe PDF

Older PDF versions derive a 40-bit key from the user supplied password. Our rainbow tables recover that key, usually in less than a minute. Once the key has been recovered, the document can be decrypted. Again, the key, not the password, is recovered. Newer PDF versions use 128-bit keys and cannot be attacked with rainbow tables.

Windows LAN Hash

These rainbow tables are a little different than the others. First, they recover passwords, not keys. Second, the number of possible LAN passwords is much more than a trillion (the approximate size of a 40-bit key space), so it is not practical to generate a complete set of LAN rainbow tables. However, if we restrict the set of characters in the passwords to letters, numbers, and about 16 other symbols, then the rainbow tables covering these passwords fit in about the same space as the Office and PDF tables.

[Return to top](#)

Contact

[Request Information](#)

[Go To Top »](#)

Products

- [Forensic Toolkit](#)
- [AD Enterprise](#)
- [AD eDiscovery](#)
- [AD Summation iBlaze](#)
- [AD Summation Enterprise](#)
- [AD Summation CaseVantage](#)
- [CIRT](#)
- [SilentRunner Sentinel](#)
- [AD Lab](#)
- [Mobile Phone Examiner Plus](#)
- [Distributed Network Attack](#)

- [Password Recovery Toolkit](#)

Support

- [AD Downloads](#)
- [Previous Releases](#)
- [Discussion Forum](#)
- [Technical Papers](#)

Resource Library

- [Brochures](#)
- [White Papers](#)
- [Webinars](#)

Training

- [AccessData Bootcamp](#)
- [AccessData Forensics](#)
- [Windows Forensics 7](#)
- [FTK 3 Transition Day](#)
- [Applied Decryption](#)
- [Internet Forensics](#)
- [Windows Forensics – XP](#)
- [Windows Forensics – Vista](#)
- [Windows Forensics – Registry](#)
- [Mobile Forensics 101](#)
- [Mobile Forensics 202](#)
- [Mobile Forensics 303](#)
- [MORE](#)

Contact Us

- [Americas/Asia Pacific](#)
- [Europe/Middle East/Africa](#)
- [Summation Software Support](#)
- [eDiscovery/Litigation Support Services](#)
- [Discovery Cracker Support](#)