



# Application Password Cracking

MODULE 12

## Contents

12.1 Learning Objectives .....	3
12.2 Application Passwords Crackers.....	3
12.2.1 Password cracking methods .....	4
12.2.1.1 Brute force attack.....	4
12.2.1.2 Dictionary attack.....	5
12.2.1.3 Syllable attack.....	6
12.2.1.4 Rule Based Attack.....	6
12.2.1.5 Hybrid attack and password guessing.....	6
12.2.1.6 Rainbow Attacks.....	6
12.2.1.7 System passwords .....	7
12.2.2 Tools for passwords cracking .....	8
12.2.2.1 CMOSPwd .....	8
12.2.2.2 ERDCommander.....	8
12.2.2.3 Office pwd recovery .....	9
12.2.2.4 Passware kit .....	9
12.2.2.5 PDF Password Crackers.....	11
12.3 Summary.....	11
12.4 Check Your Progress .....	11
12.5 Answers to Check Your Progress .....	12
12.6 Further Readings.....	12
<b>References, Article Source &amp; Contributors.....</b>	<b>12</b>

# Application Password Cracking

---

## 12.1 Learning Objectives

---

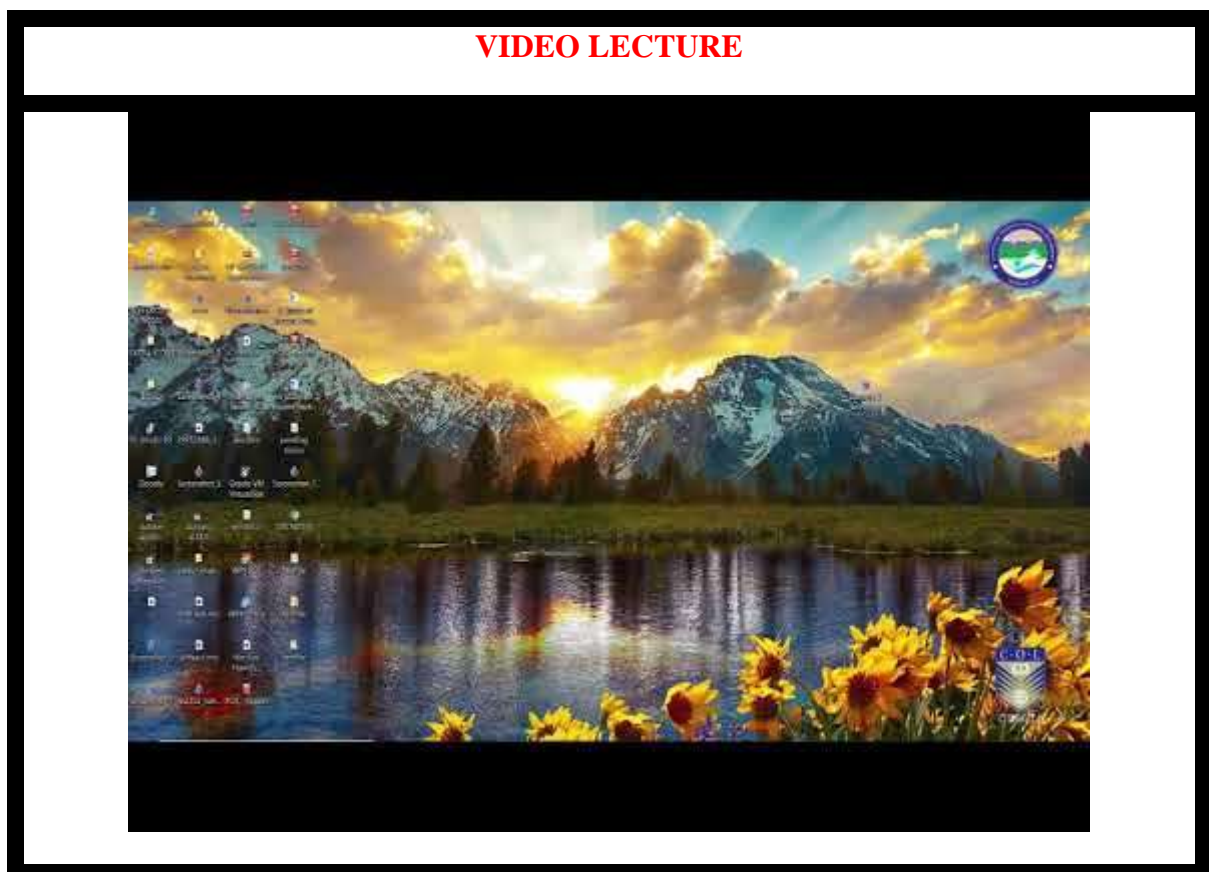
After going through this unit, you will be able to:

- Correlate basic ways how passwords are stored in Windows while doing forensic investigation.
- Perform password attacks (password hacking) and correlate while doing forensic investigation, and
- Implement various tools for password hacking useful in forensic investigation.

---

## 12.2 Application Passwords Crackers

---



A password cracker is a program that can assist users to obtain unauthorised access to an application or resources. Also, Password crackers can help users to retrieve lost or forgotten passwords of any application.

---

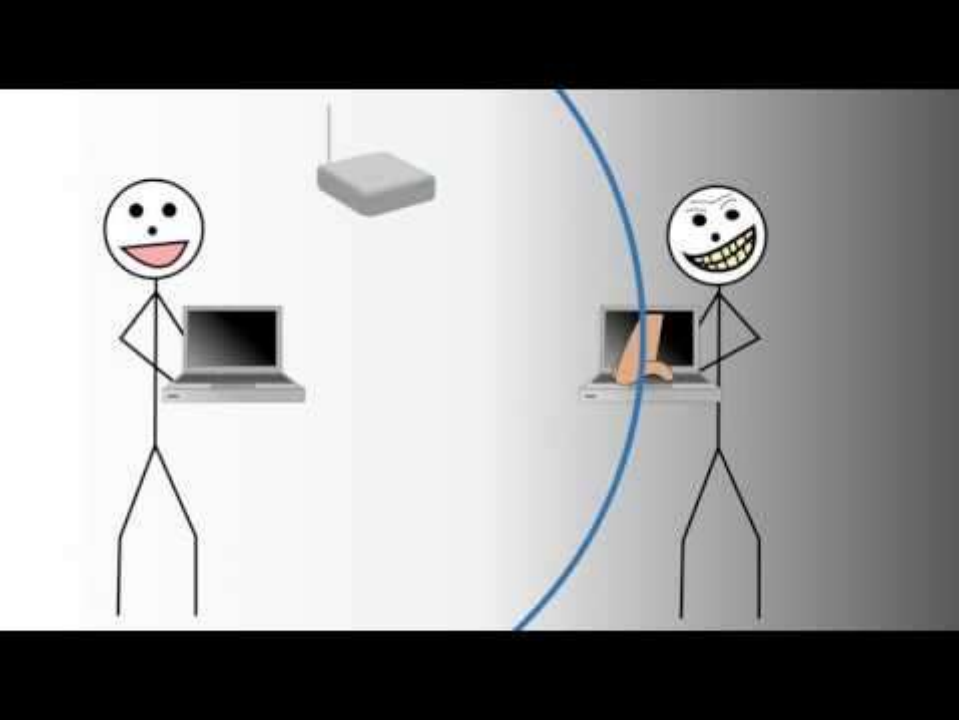
## 12.2.1 Password cracking methods

---

Password crackers can use many ways to identify a password. The most important methods are:

- a) Brute force method
- b) Dictionary searches
- c) Syllable attack
- d) Rule based attack
- e) Hybrid attack
- f) Password guessing
- g) Rainbow attack

VIDEO LECTURE



This lecture is adopted from <https://youtu.be/Mi5tFGmUtLM> available under Creative Commons Attribution license (reuse allowed);

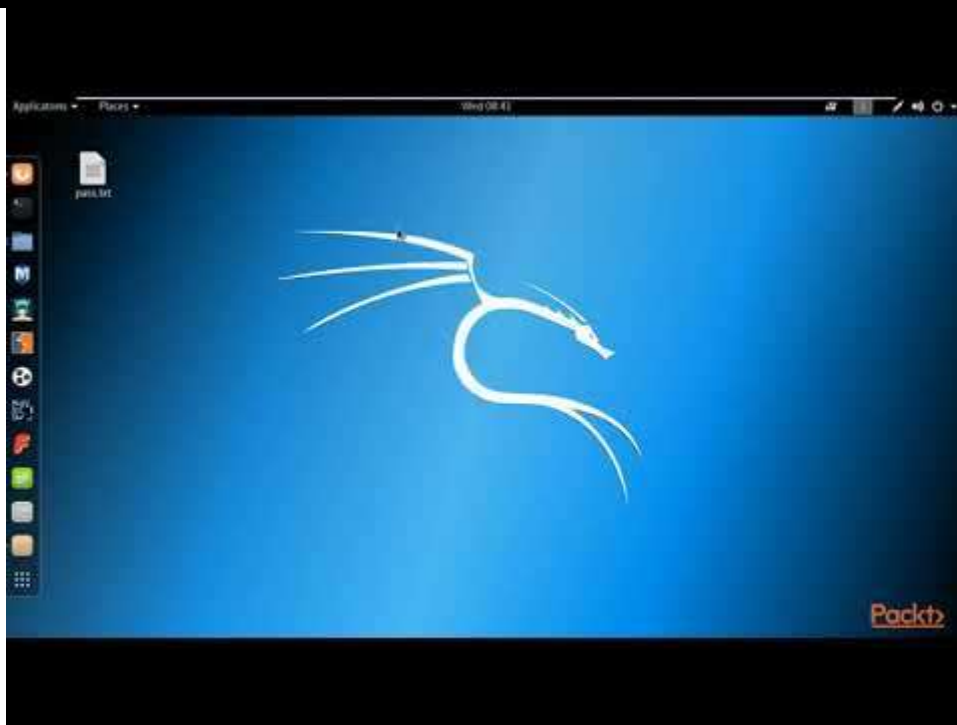
---

### 12.2.1.1 Brute force attack

---

Brute force attacks work by calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, the amount of time, on average, to find the correct password increases exponentially. This means short passwords can usually be discovered quite quickly, but longer passwords may take decades.

## VIDEO LECTURE



This lecture is adopted from <https://youtu.be/4YW4jdSW2hM> available under Creative Commons Attribution license (reuse allowed); Previous videos : <https://www.youtube.com/channel/UCfmXZF7w4CdwEUGErTgji5Q/videos>

---

### 12.2.1.2 Dictionary attack

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack. In contrast to a brute force attack, where a large proportion of the key space is searched systematically, a dictionary attack tries only those possibilities which are deemed most likely to succeed. Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords, or simple variants obtained, for example, by appending a digit or punctuation character. Dictionary attacks are relatively easy to defeat, e.g. by choosing a password that is not a simple variant of a word found in any dictionary or listing of commonly used passwords.

---

#### **12.2.1.3 Syllable attack**

---

It is a combination of the above two password attack. Many times the passwords does not contain a dictionary word and in these cases syllables form dictionary words use token and combined to every possible ways to do brute force searches.

---

#### **12.2.1.4 Rule Based Attack**

---

The attackers have many/ some preoccupied information using which the set of rules can be formed and then the possible searches can be narrowed down to a great extent. This type of attack is the most powerful one.

---

#### **12.2.1.5 Hybrid attack and password guessing**

---

It is also based on dictionary attack. In this if the old password is known than concatenating it with other symbols can yield the right password. In case of guessing the common passwords that are mostly used by novice users are used to crack codes.

---

#### **12.2.1.6 Rainbow Attacks**

---

Any computer system that requires password authentication must contain a database of passwords, either hashed or in plaintext, and various methods of password storage exist. Because the tables are vulnerable to theft, storing the plaintext password is dangerous. Most databases therefore store a cryptographic hash of a user's password in the database. In such a system, no one—including the authentication system—can determine what a user's password is simply by looking at the value stored in the database. Instead, when a user enters his or her password for authentication, it is hashed and that output is compared to the stored entry for that user (which was hashed before being stored). If the two hashes match, access is granted.

Someone who gains access to the (hashed) password table cannot merely enter the user's (hashed) database entry to gain access (using the hash as a password would of course fail since the authentication system would hash that a second time, producing a result which does not match the stored value, which was hashed only once). In order to learn a user's password, a password which produces the same hashed value must be found.

Rainbow tables are one tool that has been developed in an effort to derive a password by looking only at a hashed value.

Rainbow tables are not always needed, for there are simpler methods of hash reversal available. Brute-force attacks and dictionary attacks are the simplest methods available; However, these are not adequate for systems that use large passwords, because of the difficulty of storing all the options available and searching through such a large database to perform a reverse-lookup of a hash.

To address this issue of scale, reverse lookup tables were generated that stored only a smaller selection of hashes that when reversed could generate long chains of passwords. Although the reverse lookup of a hash in a chained table takes more computational time, the lookup table itself can be much smaller, so hashes of longer passwords can be stored. Rainbow tables are a

refinement of this chaining technique and provide a solution to a problem called chain collisions.

A rainbow table is a pre-computed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack infeasible.



---

#### 12.2.1.7 System passwords

---

Every personal computer and in that matter all computers does have a system setting or controls which are given by the hard core manufacturers to control access to system configuration and files that are vital to the boot process. In many cases users set password to the system control and there can be ways to break these passwords.

One way is to bypass the Bios password. Most of the manufacturers provide backup passwords. These can be accessed by reading their user documentation carefully. Like for example Dell gives backup password as “Dell” similarly Compaq gives as “Compaq”. However, if these backup passwords are not working one can use a combination of case sensitive back up passwords. Backup passwords are called as “Backdoor” passwords. While typing system

passwords it should be known that typing wrong passwords can lock the entire system network and render a unstable device.

Another way is by re writing the CMOS Batter. Many times, if the CMOS Battery is removed and replaced after 20-30 minutes the BIOS passwords resets.

Also, by adjusting the jumper settings on a mother board, all custom settings, including BIOS passwords will be cleaned. Location of these jumper settings may vary so we need to refer to the system documentation.

---

## 12.2.2 Tools for passwords cracking

---

There are several tools /software available to assist passwords recovery or cracking. Few examples are windows key generator, CMOSPwd, ERD commander.

---

### 12.2.2.1 CMOSPwd

---

CmosPwd decrypts password stored in cmos used to access BIOS SETUP. Works with the following BIOSes - ACER/IBM BIOS - AMI BIOS - AMI WinBIOS 2.5 - Award 4.5x/4.6x/6.0 - Compaq (1992) - Compaq (New version) - IBM (PS/2, Activa, Thinkpad) - Packard Bell - Phoenix 1.00.09.AC0 (1994), a486 1.03, 1.04, 1.10 A03, 4.05 rev 1.02.943, 4.06 rev 1.13.1107 - Phoenix 4 release 6 (User) - Gateway Solo - Phoenix 4.0 release 6 - Toshiba - Zenith AMI

---

### 12.2.2.2 ERDCommander

---

Microsoft DaRT is a successor of ERD Commander, which was part of the *Winternals Administrator Pack* from Winternals. ERD Commander later became a Microsoft property with its acquisition of Winternals on 17 July 2006.

Microsoft DaRT is based on Windows Preinstallation Environment now referred to as the Windows Recovery Environment. The tool set includes:

- Registry editor: Edits Windows Registry
- Locksmith: Resets a user account's password
- Crash Analyzer: Analyzes crash dumps
- File Restore: Restores deleted files
- Disk Commander: Repairs volumes, master boot records and partitions
- Disk Wipe: Irrecoverably erases data from hard disk
- Computer Management: A group of utilities that help retrieve system information, enable, disable or manage device drivers, Windows services and software that run during computer startup, inspect the event logs of the offline system and manage partitions.
- Explorer: A file manager
- Solution Wizard: A guidance tool that helps user choose the proper repair tool
- TCP/IP Config: Displays and modifies TCP/IP configuration
- Hotfix Uninstall: Uninstalls Windows hotfixes



- SFC Scan: Revives corrupted or deleted system files by copying them from the Windows installation source
- Search: Searches a disk for files
- Defender (formerly Standalone System Sweeper): An antivirus that scans a system for malware, rootkits, and potentially unwanted software. Uses the same engine as Microsoft Security Essentials and other Microsoft antivirus products.

ERD Commander originally included more tools, including a web browser.

---

### 12.2.2.3 Office pwd recovery

---

Office Password Recovery Toolbox is software which recovers lost password to any Microsoft Office document effectively. It can also recover read only files password. It allows several features to users letting them to set parameters to the searching password range like shape and length of the password. It enables users to search for string documents more efficiently and quickly. It recovers read only passwords from Microsoft Office Access. It is such type of application that can recover lost or forgotten password for Microsoft PowerPoint presentations, Microsoft Excel spreadsheets, Microsoft Access databases, Microsoft Outlook e-mail accounts, Microsoft OneNote notebooks etc. It can recover passwords instantly and helps in modifying sheet protection passwords, workbook passwords, email account password, database passwords etc. It has user friendly interface which helps in extracting searches. The Office Password Recovery Tool provides an efficient access to MS Office documents.

#### *Features:*

- It recovers and removes all passwords of MS Excel, MS Outlook, MS Access documents, MS Word and VBA projects.
- It is able to crack all the Office document passwords and enables them for modifying workbook and worksheet passwords (Excel only), document protection passwords, database, user work group passwords and VBA project passwords.
- The entire recently opened password protected Microsoft Office documents is unprotected by using this software and opens the start up directly.
- It can access server's unique passwords and can break MS Excel or MS Word passwords irrespective of strength and length of password.
- It has the ability for protecting Office password Recovery Toolbox with password in order to prevent unauthorized access.

---

### 12.2.2.4 Passware kit

---

Passware Kit Enterprise and Forensics Passware Kit can recover the password of up to 150 different file types. It is trade, not exactly cheap tools, but can be very useful in different circumstances. This complete electronic evidence discovery solution reports all password-protected items on a computer and gains access to these items using the fastest decryption and password recovery algorithms. Many types of passwords are recovered or reset instantly, and advanced acceleration methods are used to recover difficult passwords. Passware Kit Forensic introduces a new attacks editor, which sets up the password recovery process in the most precise way to provide the quickest decryption solution possible. The highest performance is achieved with Distributed Password Recovery, using the computing power of multiple

computers.

Passware Kit Forensic includes a Portable version that runs from a USB drive and finds encrypted files, recovers files and websites passwords without modifying files or settings on the host computer. Perform a complete encrypted evidence discovery process without installing Passware Kit on a target PC.

Passware Kit Forensic, complete with Passware FireWire Memory Imager, is the first commercial software that decrypts BitLocker and TrueCrypt hard disks of the seized computers without applying a time-consuming brute-force attack.

#### *Key Features:*

- Recovers passwords for 180+ file types and decrypts hard disks New!providing an all-in-one user interface
- Scans computers and network for password-protected files (Encryption Analyzer Professional included)
- Acquires memory images of the seized computers (FireWire Memory Imager included) New!
- Retrieves electronic evidence in a matter of minutes from a Windows Desktop Search Database (Search Index Examiner included)
- Supports Distributed and Cloud Computing password recovery New!
- Runs from a USB thumb drive and recovers passwords without installation on a target PC (Portable Version included)
- Includes 1-year Subscription to updates

#### *General Features*

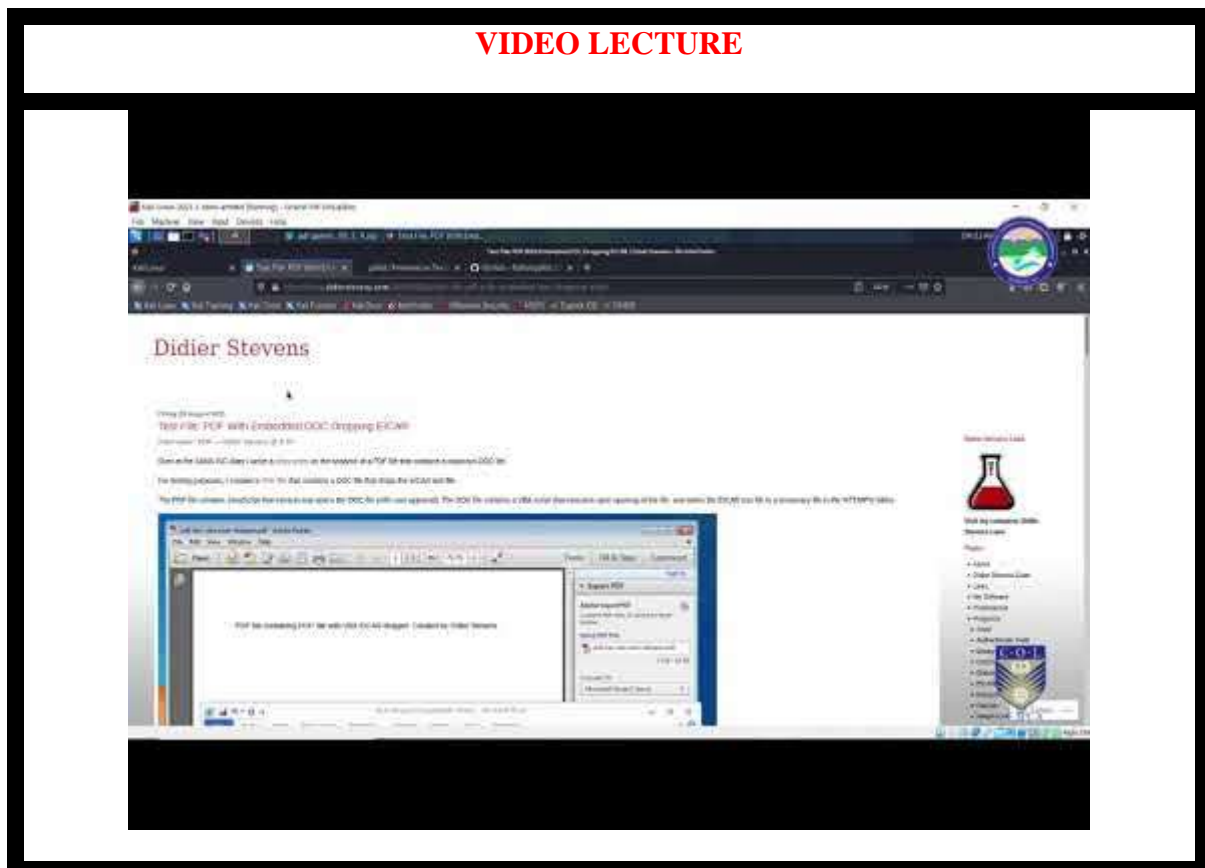
- Instantly recovers many password types
- Instantly decrypts MS Word and Excel files up to version 2003 (20 Credits for Decryptum attack included)
- Resets passwords for Local and Domain Windows Administrators instantly
- Recovers encryption keys for hard disks protected with BitLocker in minutes, including BitLocker ToGo New!
- Decrypts TrueCrypt volumes in minutes New!
- Provides 8 different password recovery attacks (and any combination of them) with an easy-to-use setup wizard and drag & drop attacks editor
- Uses multiple-core CPUs and NVIDIA GPUs efficiently to speed up the password recovery process by up to 45 times
- Uses Tableau TACC hardware accelerators to speed up the password recovery process by up to 25 times
- Provides detailed reports with MD5 hash values

---

### 12.2.2.5 PDF Password Crackers

---

CrackPDF, Abcom PDF Password Cracker, and Advanced PDF Password Recovery can all be used to access password-protected Adobe PDF files. CrackPDF and Abcom PDF Password Cracker use brute force attacks to discover the passwords, while Advanced PDF Password Recovery simply removes the password protection entirely.



---

## 12.3 Summary

---

1. User and passwords in a window system are stored in either Security Account Manager or Activity directory.
2. The most important methods of password cracking are brute force method, dictionary searches, syllable attack, rule based attack, hybrid attack, password guessing, rainbow attack.
3. There are several tools /software available to assist passwords recovery or cracking. Few examples are windows key generator, CMOSPwd, ERD commander.

---

## 12.4 Check Your Progress

---

1. State True or False

- a) The Security Account Manager (SAM) is a database file in Windows.

- b) Office Password Recovery Toolbox is software which stores lost password to any Microsoft Office document effectively.
- c) Non-wrapping can occur when the event log is created or when the event log is cleared.

---

## 12.5 Answers to Check Your Progress

---

### 1. State True or False

- a) True
- b) False
- c) True

---

## 12.6 Further Readings

---

1. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
2. Investigating Hard Disks, File and Operating Systems: EC-Council | Press
3. Windows Event Log (EVT) – ForensicsWiki, [www.forensicswiki.org/wiki/Windows\\_Event\\_Log\\_\(EVT\)](http://www.forensicswiki.org/wiki/Windows_Event_Log_(EVT))
4. Audit User Account Management - TechNet – Microsoft, [https://technet.microsoft.com/en-us/library/dd772693\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd772693(v=ws.10).aspx)
5. Event Log File Format (Windows) - MSDN – Microsoft, [https://msdn.microsoft.com/en-us/library/windows/desktop/bb309026\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb309026(v=vs.85).aspx)
6. Policy Change - TechNet – Microsoft, [https://technet.microsoft.com/en-us/library/dd772669\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd772669(v=ws.10).aspx)
7. Reading from the Event Log (Windows) - MSDN – Microsoft, [https://msdn.microsoft.com/en-us/library/windows/desktop/aa363675\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa363675(v=vs.85).aspx)

## References, Article Source & Contributors

- [1] Active Directory - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Active\\_Directory](https://en.wikipedia.org/wiki/Active_Directory)
- [2] CMOSPwd, <https://packages.gentoo.org/packages/app-forensics/cmospwd>
- [3] Dictionary attack - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Dictionary\\_attack](https://en.wikipedia.org/wiki/Dictionary_attack)
- [4] Event logging – Wikipedia, [https://en.wikipedia.org/wiki/Event\\_logging](https://en.wikipedia.org/wiki/Event_logging)
- [5] Log analysis - Wikipedia, the free encyclopedia, [https://en.wikipedia.org/wiki/Log\\_analysis](https://en.wikipedia.org/wiki/Log_analysis)
- [6] logparser - Wikipedia, the free encyclopedia, <https://en.wikipedia.org/wiki/Logparser>
- [7] Microsoft Desktop Optimization Pack - Wikipedia, [https://en.m.wikipedia.org/.../Microsoft\\_Diagnostics\\_and\\_Recovery\\_Tool](https://en.m.wikipedia.org/.../Microsoft_Diagnostics_and_Recovery_Tool)
- [8] Passware kit, [http://azizalstsetia.blogspot.in/2011/04/passware-kit-forensic-103-full-version\\_7549.html](http://azizalstsetia.blogspot.in/2011/04/passware-kit-forensic-103-full-version_7549.html)

- [9] Password cracking - Wikipedia, the free encyclopedia,  
[https://en.wikipedia.org/wiki/Password\\_cracking](https://en.wikipedia.org/wiki/Password_cracking).
- [10] Rainbow table - Wikipedia, the free encyclopedia,  
[https://en.wikipedia.org/wiki/Rainbow\\_table](https://en.wikipedia.org/wiki/Rainbow_table)
- [11] Recover lost MS Office Password, [recoverlostofficepassword.wikidot.com](http://recoverlostofficepassword.wikidot.com)
- [12] Security Account Manager - Wikipedia, the free encyclopedia,  
[https://en.wikipedia.org/wiki/Security\\_Account\\_Manager](https://en.wikipedia.org/wiki/Security_Account_Manager)
- [13] Windows XML Event Log, (EVTX),  
[http://www.forensicswiki.org/wiki/Windows\\_XML\\_Event\\_Log\\_\(EVTX\)](http://www.forensicswiki.org/wiki/Windows_XML_Event_Log_(EVTX))

## **EXPERT PANEL**



**Dr. Jeetendra Pande, Associate Professor- Computer Science, School of  
Computer Science & IT, Uttarakhand Open University, Haldwani**



**Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and  
Energy Studies, Dehradun**



**Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy  
Studies, Dehradun**



**Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of  
Engineering, Kaman, Vasai, University of Mumbai**



**Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert**



**Ms. Priyanka Tewari, IT Consultant**



**Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharashtra**



**Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani**



**Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar**



This MOOC has been prepared with the support of



© Commonwealth Educational Media Centre for Asia , 2021. Available in Creative Commons Attribution-ShareAlike 4.0 International license to copy, remix and redistribute with attribution to the original source (copyright holder), and the derivative is also shared with similar license.