

DATA COMPROMISE ASSESSMENT



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DISCLAIMER

This document does not promote or encourage any illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.



INTRODUCTION TO DATA LEAKAGE ANALYZER

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



INTRODUCTION TO DATA LEAKAGE ANALYZER

Data protection is important, critical, vital. Loss of data can play havoc in many ways. It can be disastrous. Cybercriminals steal data, use that data for stealing money and for conducting further breaches. Loss of data affects privacy and security. Data has grown up massively in terms volume. Data has value and if it falls into the wrong hands it can have drastic consequences. There have been sensitive data breaches earlier, but they have become more frequent nowadays.



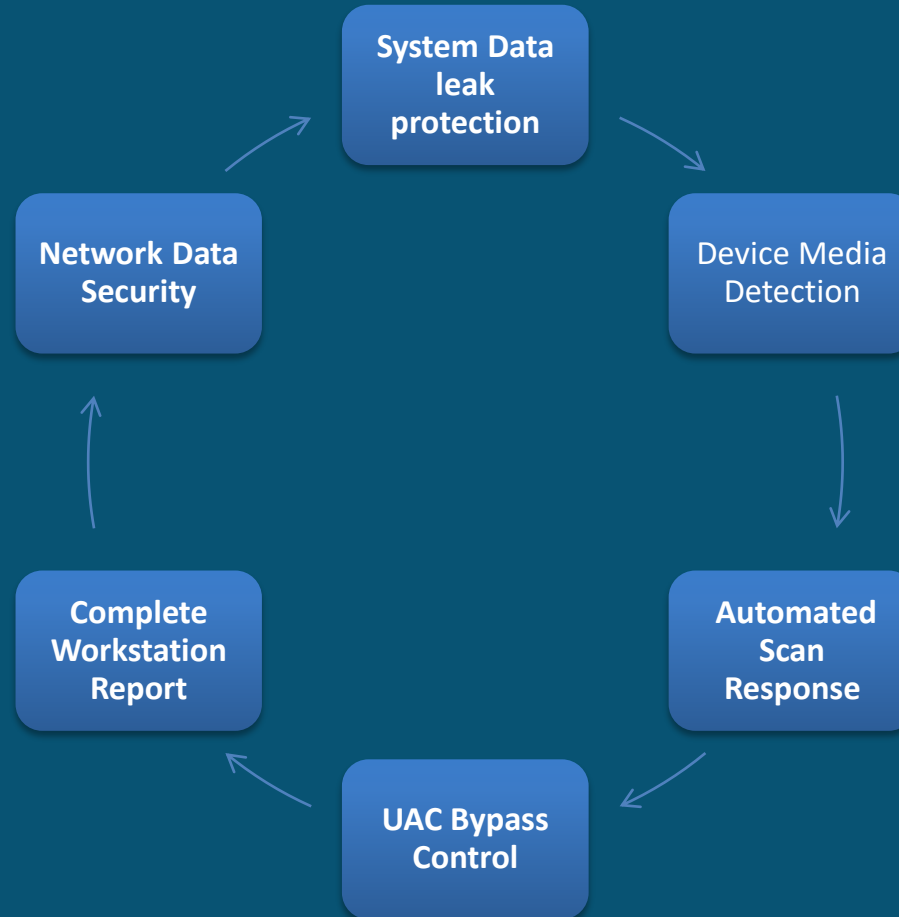
INTRODUCTION TO DATA LEAKAGE ANALYZER

- Enforcement of DLP technology enables monitoring of the location and usage of data according to the laid out DLP policies.
- DLP can help prevent accidental disclosure or theft by employees having access to sensitive data. Internal employees have access to sensitive data, and hence their corporate communication, browsing, etc., are events to be monitored. Non-productive and data risky activities must be blocked.
- DLP can help prevent lawsuits, loss of reputation, loss of credibility, loss of revenue.
- Allowing BYOD has increased the vulnerability of data loss. As BYOD and mobile devices are there to stay for enterprises, it would be better for the enterprise to implement a robust Mobile Device Management system along with DLP technologies.
- Data security events must be captured as they may be required for forensic analysis and proof of inappropriate employee misconduct.
- Most enterprises are storing data in the cloud. This too has become risky with many malicious malware targeting data in the cloud.
- DLP technology automatically encrypts confidential data to prevent data loss.



INTRODUCTION TO DATA LEAKAGE ANALYZER

KEY FEATURES



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER COMPLETE FEATURES

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

DASHBOARD

A Single Dashboard for all your security Audit , includes complete set of features and a holistic view for the user to quickly and easily access various features of the Data Leakage Assessment Through which the user can gain a result oriented work. Following are the few data the software collects in seconds to help auditor quickly assess the system ; Machine Name , Machine Serial , OS type , Windows Version , Available RAM, Total RAM , MAC Address , Installation Date , Is USB Enabled , Local IP Address , Public IP Address , Is Windows Activated . The Dashboard also provides options for the Auditor to change the settings as preferred and also is able to check the updates for the system and built-In Protection for the System in case of any threats . U can also use the software to save results of the automated software in txt file.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

DASHBOARD

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

DLP Dashboard
Local File Server
File Transfer Via Web
UAC Bypass
Detected Media Type
Stored Passwords
Recent System History
Wifi Profiles
Bit Locker Statu

<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>File Transfer Via Web</p> <p>Allowed</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Removeable Media</p> <p>Allowed</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Local File Server Permission</p> <p>Not Allowed</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Stored Passwords</p> <p>Found</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Addons / Plugins</p> <p>Found</p> </div>
<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Internet Connectivity</p> <p>Allowed</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Wifi Profiles</p> <p>2</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>User Account Control</p> <p>Not Allowed</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; text-align: center;"> <p>Recent Items</p> <p>2519</p> </div>	

Scan System
Protect System
Reset Setting
Check for Updates
Save Results

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

LOCAL FILE SERVER

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Status](#)

File Sharing Server

Local IP Address 192.168.1.16
Port

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE ANALYZER

COMPLETE FEATURES

LOCAL FILE SERVER

Securely track the File Servers for access, changes to the documents in their files and folder structure, shares and permissions. View from the exclusive file audit reports with 50+ search attributes and filter based on user / file server / custom / share based reporting for crisp detailed information.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

FILE TRANSFER VIA WEB

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Status](#)

Domain: <https://filetransfer.io/> Allowed for File Transfer
 Domain: <https://web.whatsapp.com/> Allowed for File Transfer
 Domain: <https://transferl.com/> Allowed for File Transfer
 Domain: <https://www.mailbigfile.com/> Allowed for File Transfer

[Scan System](#)
[Protect System](#)
[Reset Setting](#)
[Check for Updates](#)
[Save Results](#)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

FILE TRANSFER VIA WEB

Displays the different domains used for the transfer of files from the local network



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

UAC BYPASS

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Status](#)

Install App

Trying UAC Bypass:
UAC BYPASS SUCCESSFULLY

[Scan System](#)
[Protect System](#)
[Reset Setting](#)
[Check for Updates](#)
[Save Results](#)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

UAC BYPASSSS

Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. This application shows if it is successful or not .



DATA LEAKAGE ANALYZER


COMPLETE FEATURES

DETECTED MEDIA TYPE

Data Leakage Analyzer - v2.0
— □ ×

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

DLP Dashboard | Local File Server | File Transfer Via Web | UAC Bypass | Detected Media Type | Stored Passwords | Recent System History | Wifi Profiles | Bit Locker Statu



Is USB Enabled | Enabled
 CD-ROM :PLDS DVD-RW DS8A9SH
 Fixed
 Fixed
 CDRom

Scan System
Protect System
Reset Setting
Check for Updates
Save Results

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

DETECTED MEDIA TYPE

Displays the type of media enabled for connection establishment.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

STORED PASSWORDS

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	4953 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Statu](#)

Origin URL : <https://brilliant.org/account/signup/>
 Action URL : <https://brilliant.org/account/signup/>
 User Name Field : email
 Password Field : password1
 User Name : wekikoj627@maillei.net
 Password : wekikoj627@maillei.net
 Created Time : 9/24/2020 1:06:25 PM
 Password Strength : Very Weak
 Password File : C:\Users\BlackWin\AppData\Local\Google\Chrome\User Data\Default>Login Data
 =====
 =====
 Origin URL : <https://login.yahoo.com/>

[Scan System](#)
[Protect System](#)
[Reset Setting](#)
[Check for Updates](#)
[Save Results](#)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE ANALYZER

COMPLETE FEATURES

STORED PASSWORDS

Captures all the passwords saved in the machine with the website name , time for last modified , password strength , file path .

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

RECENT SYSTEM HISTORY

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Statu](#)

←

```

=====
-----
Filename      : C:\Users\Black Win\Desktop\recyclebin.PNG
Modified Time  : 9/22/2020 5:58:55 PM
Created Time   : 9/22/2020 5:58:55 PM
Execute Time   : 9/22/2020 6:02:57 PM
Missing File   : Yes
Stored In      : Recent Folder
Extension      : PNG
File Only      : recyclebin.PNG
=====
-----
    
```

[Scan System](#)
[Protect System](#)
[Reset Setting](#)
[Check for Updates](#)
[Save Results](#)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE ANALYZER

COMPLETE FEATURES

RECENT SYSTEM HISTORY

Complete Display if the user has made any changes in the system for example making changes in the file names or using extensions or patches to create or breach data in order to gain unauthorized access to the system.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

WIFI PROFILES

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

[DLP Dashboard](#)
[Local File Server](#)
[File Transfer Via Web](#)
[UAC Bypass](#)
[Detected Media Type](#)
[Stored Passwords](#)
[Recent System History](#)
[Wifi Profiles](#)
[Bit Locker Status](#)

All User Profile : Virtual-Security
 All User Profile : Virtual-Core

[Scan System](#)
[Protect System](#)
[Reset Setting](#)
[Check for Updates](#)
[Save Results](#)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

WIFI PROFILES

Shows the connection of the machine on different networks it has connected with and is able to track any type of network including ADHOC network incase of any theft.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

BIT LOCKER STATUS

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	4190 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

Local File Server | File Transfer Via Web | UAC Bypass | Detected Media Type | Stored Passwords | Recent System History | Wifi Profiles | **Bit Locker Status** | Allowed Extensions

Win32_EncryptableVolume instance
BitLocker Disabled

Scan System | Protect System | Reset Setting | Check for Updates | Save Results

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

BIT LOCKER STATUS

The software indicates that BitLocker is not available on the device. BitLocker needs to first be available on the device (TPM and BIOS), and additionally must meet minimum requirements defined by Microsoft.



DATA LEAKAGE ANALYZER

COMPLETE FEATURES

ALLOWED EXTENSIONS

Data Leakage Analyzer - v2.0

Machine Name	CS-R1	Available RAM	5021 MB	Is USB Enabled	Enabled
Machine Serial	MJ00DXKP	Total RAM	8364683264	Local IP Address	192.168.1.16
Operating System	Microsoft Windows NT 6.2.9200.0	MAC Address	02004C4F4F50	Public IP Address	39.51.117.177
Windows Version	4.0.30319.42000	Installation Date	8/18/2019, 3:29:28 AM	Is Windows Activated	0.0.0.0

File Transfer Via Web | UAC Bypass | Detected Media Type | Stored Passwords | Recent System History | Wifi Profiles | Bit Locker Status | **Allowed Extension**

Item ID : aapocclcgogkmnckokdopfmhonfmgok
 Status : Enabled
 Web Browser : Chrome
 Addon Type : Extension
 Name : Slides
 Version : 0.10
 Description : Create and edit presentations
 Title :
 Creator :
 Install Time : 8/18/2019 9:10:40 PM
 Update Time :
 Homepage URL :

Scan System | Protect System | Reset Setting | Check for Updates | Save Results

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE ANALYZER

COMPLETE FEATURES

ALLOWED EXTENSIONS

Microsoft hides file extensions in Windows by default even though it's a security risk that is commonly abused by phishing emails and malware distributors to trick people into opening malicious files. To Prevent Leaks, Breaches, Hacks & Insider Threats Before They Take Root, our software helps detect the file type and gather information of user activity over the browser.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



DATA LEAKAGE SCENARIOS

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE SCENARIOS

WORKGROUP / NON DOMAIN MACHINE

When a Machine is plugged in an organization premises and does not belong to the organization. The organization may reserve the right to confiscate the machine and search it in the same premises. Following are the list of possible ways and the tools on which compromised data can be identified from a WORKGROUP / NON Domain machine which has been confiscated.

Conducting Live **Data Compromise Assessment (DCA)**:

Reference: <https://www.nirsoft.net/utils>

S. No	Control Name	Description	Tool / Technique
1	Search for Last Activity View	Windows operating system that collects information from various sources on a running system, and displays a log of actions made by the user and events occurred on this computer. The activity displayed by LastActivityView includes: Running .exe file, Opening open/save dialog-box, Opening file/folder from Explorer or other software, software installation, system shutdown/start, application or system crash, network connection/disconnection and more	 lastactivityview.zip
2	Searching for Suspicious Apps	Search Suspicious app such as (Tor, Torrent, VNC, RATS, TROJANS, Malwares) etc. in the system	
3	Search for Browsing History	Collect history data of different Web browsers (Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera) and displays the browsing history of all these Web browsers in one table. The browsing history table includes the following information: Visited URL, Title, Visit Time, Visit Count, Web browser and User Profile.	 browsinghistoryview-x64.zip

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.







DATA LEAKAGE SCENARIOS

WORKGROUP / NON DOMAIN MACHINE

When a Machine is plugged in an organization premises and does not belong to the organization. The organization may reserve the right to confiscate the machine and search it in the same premises. Following are the list of possible ways and the tools on which compromised data can be identified from a WORKGROUP / NON Domain machine which has been confiscated.

Conducting Live **Data Compromise Assessment (DCA)**:

Reference: <https://www.nirsoft.net/utils>

S. No	Control Name	Description	Tool / Technique
4	Search for Downloaded Data from Browsers	BrowserDownloadsView allows you to load the downloads list from your current running system (your user or all user profiles), from remote computer on your network , and from external hard drive.	 browserdownloadsview-x64.zip
5	Open/Save File View	View list of List which has been opened or saved in the system.	 opensavefilesview-x64.zip
6	Collect USB Logs	Get list of USB Connected with the current system along with Vendor name, date/time and USB type.	 usbdeview-x64.zip
7	Search for Prefetch Items	A Prefetch file which contains information about the files loaded by the application is created by Windows operating system	 winprefetchview-x64.zip

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.





DATA LEAKAGE SCENARIOS

WORKGROUP / NON DOMAIN MACHINE

When a Machine is plugged in an organization premises and does not belong to the organization. The organization may reserve the right to confiscate the machine and search it in the same premises. Following are the list of possible ways and the tools on which compromised data can be identified from a WORKGROUP / NON Domain machine which has been confiscated.

Conducting Live **Data Compromise Assessment (DCA)**:

Reference: <https://www.nirsoft.net/utils>

S. No	Control Name	Description	Tool / Technique
8	Shall Bag Analyze	List of all folder settings saved by Windows. For each folder, the following information is displayed: The date/time that you opened it, the entry number, display mode (Details, Icons, Tiles, and so on...), the last position of the window, and the last size of the window.	 shellbagsview.zip
9	Jump List	When analyzing a Windows computer is that Jump Lists are indicative of user activity. Essentially Jump Lists track files accessed by a user, therefore they will assist in most examinations where a user's actions on the computer are the focus of the analysis.	Go to Run > %Userprofile%\AppData\Roaming\Microsoft\Windows\Recent\
10	User Assist View	This utility decrypt and displays the list of all UserAssist entries stored under HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist key in the Registry. The UserAssist key contains information about the exe files and links that you open frequently.	 userassistview.zip

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



THANK YOU

