# CHAPTER I

# INTRODUCTION

The password has been used to encrypt the information or message for a long time in the history and it leads to discipline: cryptography, Furthermore, with the rapid development of computer science, the passwords is now also commonly used for user authentication issue, which is very important to the internet security.

RFC 2828 defines user authentication as “the process of verifying an identity claimed by or for a system entity”. The authentication service must assure that the connection is not interfered with by a third party masquerading as one of the two legitimate parties, which usually concerns two approaches data origin authentication. The data origin authentication provides for the corroboration of the source of the source of a data unit without the protection against the duplication or modification of data units, and this type of service supports applications like email where there are no prior interactions between the communicating entities. The peer entity authentication provides for the corroboration of the identity of a peer entity in an association for use of a connection at the establishment or at times during the data transfer phase, which attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection. There are usually four means of authenticating user identity based on: something the individual know (e.g. password, PIN, answers to prearranged questions). Something the individual does (token e.g: smartcard, electronic keycard, physical key). Something the individual is (static biometrics, e.g. fingerprint, retina, face), .The growth of both IT technology and the Internet Communication has involved the development of lot of encrypted information. Among others techniques of message hiding, stenography is one them but more suspicious as no one cannot see the secret message. As we always use the MS Office, there are many ways to hide secret messages by using PowerPoint as normal file. Owing to a number of reasons, the deployment of encryption solutions are beginning to be ubiquitous at both organizational and individual levels. The most emphasized reason is the necessity to ensure confidentiality of privileged information. Unfortunately, it is also popular as cyber-criminals' escape route from the grasp of digital forensic investigations. The direct encryption of data or indirect encryption of storage devices, more often than not, prevents access to such information contained therein.[1]

Data is becoming largely existent in today's world than they were anticipated some three decades ago. Individuals are keeping lot more amount of information than organizations kept in the yesteryears. Significant amounts of such information are valued and consequently preferred to be known to them alone. Such valued information includes their financial details, medical records, locations, as well as professional and network information. Businesses and organizations possess larger amounts of information than individuals. A good amount of such information is critical to their sustained existence and growth. Their intellectual properties and trade secrets are kept away from potential exploits, thus, considered very private. Governments and agencies keep sensitive information that may affect the stability of their jurisdictions, politically or economically, if divulged. The necessity to keep such information within the required confines describes a component purpose of Information Security, which involves the totality of activities to ensure the protection of information assets that use, store, or transmit information from risk through the application of policies, education, training, awareness, and technology. Data security involves the consideration of potential confidentiality, integrity, and availability threats to data services, using functions such as identification, authentication, authorization and audit. Data encryption may not be an explicit solution to information security problems, as organizations remain increasingly vulnerable to data breach incidents, but it is still the most efficient fix when deployed adequately . This has led to the growing availability of full disk encryption tools. Disk manufacturers are embedding full encryption tools into their products, making encryption more available for use. The study conducted by showed the increased usage of full disk, virtual volume, native disk, and flash drive encryptions over two years. However, for reasons other than the cost of deployment and managing an encryption solution, some organizations have shunned or still undecided about adopting encryption solutions. They insisted that “availability is more important than confidentiality”. [10]

Surveys revealed the continuously increasing adoption of cryptographic solutions by organizations for various data security platforms within the last five years. The report of the surveys infers the anticipation of non-users to adopt partial or holistic cryptographic solutions in the nearest future. This suggests the impending domination by cryptographic procedures, to protect information in the computer world. There are ways for investigators to out maneuver the use of cryptography as a provocation to digital forensics processes. These methods are either by legally obtaining appropriate 'search and seize' authorizations or tactically planning to catch the offender unawares and hence, access live – running and unencrypted – systems . However, only a handful of encryption incidents encountered by investigators have been solved using those methods. The larger lot of about 60% often does not get prosecuted, not because they were missed, but because nothing could be done to access the potential evidence . The inconsistency of legal systems across boundaries does not make the process easier, as laws may or may not enjoin perpetrators to help the investigators access the encrypted medium . This was evident in the Dantas' suspected money laundering case, where Brazil had no legislation to make him reveal his passphrase or encryption type, unlike the United Kingdom . Therefore, researchers and developers need to be reminded of privacy-enforcement threats to forensic investigations, and pestered about the need for technologies to help deal with accessing encrypted storage devices.

Data Encryption for Information Security In order to examine threats contributed by a technology, the solutions it offers should be considered too. Encryption, as an element of cryptography, is a methodology for achieving information security, through secretive communications. The United Kingdom's Data Protection Act 1998 most suitably describes the confidentiality element of information security. It seeks to ensure that the information held by organizations of their customers and employees are safeguarded from other uses than they were obtained . This is meant to avert incidents such as identity crimes, and protect such potential victims from damages and embarrassment that unauthorized use of their data may cause the powers conferred on the Information.

There is also a huge necessity to ensure the confidentiality of data items, at rest, in use, or in motion. Financial organizations, where transactions are regularly performed on data, have to ensure that such data are not subject to unauthorized access or modifications. The combination of the encryption and hash technologies to create digital signatures and certificates, which are used to ensure data confidentiality and integrity, is a laudable approach. As far as information security is concerned, data encryption technology has been of invaluable success on the confidentiality and integrity fronts. Whereas on the availability front, it is known for delays on sparse occasions. Serious availability issues caused by the deployment of encryption solutions are not unheard of, although they are usually addressable by providers . In an overall sense, it is hence, agreeable to regard data encryption as a massive solution for information security challenges. DumpIt is a compact portable tool which makes it easy to save the contents of your PC's RAM. It's a console utility, but there's no need to open a command line, or master a host of cryptic command line switches. Instead, all you do is double-click the program's executable (a tiny 203 KB), press "Y" to confirm that you're "sure you want to continue" - and that's it, DumpIt will save the contents of RAM to a file in DumpIt's current folder course this may take a while, especially if you've a lot of RAM. DumpIt will save your entire 3GB user address space on a 32-bit Windows system, and the contents of your entire installed RAM on a 64-bit system, so this isn't going to happen in a second or two. Be patient, though, and the DumpIt window will alert you when the process is complete. Dump the RAM to disk, use something like the hex editor HxD to open the file, and you can search for a phrase which you know was in the text. With any luck you'll find it (we tested this with Word 2010 and it worked just fine), and while you won't be able to copy and paste the text from RAM, or easily extract images or binary data, you can at least read it and retype the text elsewhere. Alternative, MoonSols Windows Memory Toolkit can take a memory dump and convert it into a form which can be analyzed by Microsoft Windows Debugger, which may (for example) help you to figure out why your troublesome program locked up in the first place. Read more at the MoonSols site.

DumpIt provides an easy way to save the contents of RAM. This probably isn't something you'll need to use often, but when you do then it could be very useful, and as the program is also small and portable then it's well worth putting aside for emergencies [13]

The research completely on the task of capturing images using dumpIt version 3.2 and cracking password using AccessData_FTK_Imager_4.2.1 (FTK). And study the free version of this software is how much accurate to get the results by examine with ten personal computers physical memory in live. By the study relating to get to know how much the ordinary person capturing the image of the system USING dumpIt and cracking passwords with FTK. This study giving the clear cut view how the forensic examing tool is FTK and dumpIt.

The effectiveness of data encryption as a mechanism for enforcing information privacy is massive. This is evident by the reported widespread use of various data encryption solutions at the organizational and individual levels. However, its huge success for data access restriction has been a threat for digital forensics processes over the years. Cyber-criminals have been exploiting the information confidentiality ability of data encryption solutions, to restrict digital forensics investigators' accesses to potential evidence. The ubiquitous availability, inexpensive cost and easy implementation of encryption solutions enhance the threats posed to digital forensics processes. Investigators sometimes get around the encryption challenge through careful and thoughtful planning of search and seizure, thorough search for exposed encryption keys, and advanced in memory data retrieval techniques. Yet, a minimum of 60% of computer incidents involving data-encryption end up not prosecutable[11]

# CHAPTER II

# LITERATURE REVIEW

Basic Technology Corporation (2008) “October version 2.20 and now the latest version 4.14.0 of Autopsy” Autopsy is a GUI-based open source digital forensic program to analyze hard drives and smart phones efficiently. Autospy is used by thousands of users worldwide to investigate what happened in the computer. Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card. Training and Commercial Support are available from Basis Technology. Easy to Use Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details. Extensible, Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
  □Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

Fast everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the fast results page for more details .Cost Effective, freeware. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis that other commercial tools do not provide. It's widely used by corporate examiners, military to investigate and some of the features are. Email analysis, File type detection, Media playback Registry analysis Photos recovery from memory card, Extract geolocation and camera information from JPEG files ,Extract web activity from browser Show system events in graphical interface Timeline analysis, Extract data from Android – SMS, call logs, contacts, etc. It has extensive reporting to generate in HTML, XLS file format.

Jad (2011) "Magnet RAM Capture" was helping a lot of the people he had shared it with, and he wanted to bring more features and capabilities to IEF. He was introduced to help build a company that was smart and doing good in the world. Together, they launched Magnet RAM capture to capture the physical memory of a computer and analyze artifacts in memory. Acquiring Memory with Magnet RAM Capture Recently, released a new free tool that allows investigators to acquire the memory of a live PC. Customers using our IEF Triage module will already be familiar with this tool, as it's used to acquire evidence from live systems. In realizing that others could benefit from our RAM capture tool, to release it free to the forensics community .Memory analysis can reveal a lot of important information about a system and its users. There are often instances where evidence stored in memory is never written to the hard drive, and may only be found in the pagefile.sys or hiberfil.sys. Memory analysis is essential to many malware and intrusion incidents and can be imperative in recovering valuable evidence for almost any PC investigation. Running processes and programs, active network connections, registry hives, passwords, keys and decrypted files are just a few examples of the evidence that can be found in memory. Many web apps, like Gmail, or private/incognito browsing modes will only store data in memory meaning the evidence cannot be recovered from the hard disk .Magnet RAM Capture supports both 32 and 64 bit Windows systems including XP, Vista, 7, 8, 10, 2003, 2008, and 2012. It will acquire the full physical memory quickly and leave a small footprint on the live system being analyzed. For my system it took about 3 minutes to image an 8 GB RAM dump. Running Magnet RAM Capture is very straightforward. The standalone executable can be run from either a USB stick or from the local machine. Users will need to specify two items prior to starting acquisition where to save the captured data, and whether the files should or should not be fragmented. Fragmentation is turned off by default, however, if you are running the utility from a FAT32 formatted USB stick and the host RAM you are capturing is greater than 4 GB, then we recommend fragmenting your files to adhere to the FAT32 maximum file size limitation. Magnet RAM Capture creates a raw data dump with a .DMP extension. If you are saving the image back to the USB, you'll want to ensure that there is enough space for the acquired memory. Once the location and segment size has been selected, you can hit start and the utility will begin capturing the system's memory. A progress bar will provide the investigator with the status of the collection. Once the collection is complete, the captured memory can be analyzed with your favorite memory analysis tool .Since the memory collected by the utility is stored in a raw data format, it can be analyzed by most memory analysis and forensic tools including IEF, Volatility, and Mandiant Redline. To analyze the memory dump with IEF, select Images from the main IEF screen and upload the raw .DMP file acquired with Magnet RAM Capture .IEF will load the RAM dump and perform a sector level search (by default) since there is no file system associated with the unstructured raw data Once loaded, you may select which artifacts you wish to include in your search (searching for everything will yield the most complete results) and begin your search just like any other image file being loaded. Upon completion of the IEF search, Report Viewer will display any artifacts found within your memory dump. Because Images was selected when the RAM dump was loaded, IEF will report any evidence it finds as a physical sector. If you want to see the results as a file offset, choose Files & Folders when loading the .DMP file and it will adjust to which ever value you prefer. Physical memory stores a wealth of information, and capturing memory from a live system should be a part of any investigator's workflow. Whether you're working a malware infection, intrusion incident, or IP theft, there is bound to be evidence found in memory that could be vital to your investigation. Magnet RAM Capture is a fast, free tool that can be added to your toolkit and it works great with your favorite memory analysis tools.

Belkasoft (2002) design RAM Capturer; is a free tool to dump the data from computer's volatile memory. It's compatible with Windows OS. Memory dumps may contain encrypted volume's password and login credentials for web mails and social network services. Belkasoft Live RAM Capturer is a tiny free forensic tool that allows to reliably extract the entire contents of computer's volatile memory – even if protected by an active anti-debugging or anti-dumping system. Separate 32bit and 64-bit builds are available in order to minimize the tool’s footprint as much as possible. Memory dumps captured with Belkasoft Live RAM Capturer can be analyzed with Live RAM Analysis in Belkasoft Evidence Center. Belkasoft Live RAM Capturer is compatible with all versions and editions of Windows including XP, Vista, Windows 7, 8 and 10, 2003 and 2008 Server.Memory dumps are a valuable source of ephemeral evidence and volatile information. Memory dumps may contain passwords to encrypted volumes (TrueCrypt, BitLocker, PGP Disk), account login credentials for many webmail and social network services such as Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; file sharing services such as Dropbox, Flickr, SkyDrive, etc. In order to extract ephemeral evidence out of already captured memory dumps, forensic experts must use proper analysis software such as Belkasoft Evidence Center. Besides, some other tools can be used to extract passwords to encrypted volumes (e.g. Elcomsoft Forensic Disk Decryptor).Acquiring volatile memory from a computer running a debugging protection or anti-dumping system is tricky. Most memory acquisition tools run in the system’s user mode, and are unable to bypass the defense of such protection system (which run in the systems’ most privileged kernel mode).Belkasoft Live RAM Capturer is designed to work correctly even if an aggressive anti-debugging or anti-memory dumping system is running. By operating in kernel mode, Belkasoft Live RAM Capturer plays on the same level with these protection systems, being able to correctly acquire address space of applications protected with the most sophisticated systems such as nProtect GameGuard. Creates Forensically Sound Memory Dumps Belkasoft Live RAM Capturer features the smallest footprint possible, does not require installation and can be launched in seconds from a USB flash drive. Unlike many competing tools running in system’s user mode, Belkasoft Live RAM Capturer comes equipped with 32-bit and 64-bit kernel drivers allowing the tool to operate in the most privileged kernel mode. Memory dumps acquired with Belkasoft Live RAM Capturer can be then analyzed with Belkasoft Evidence Center Live RAM Analysis. Compared to Other Volatile Memory Capturing Tools Belkasoft Live RAM Capturer beats many popular memory dumping applications hands down due to the difference in design goals. Current versions of competing tools (AccessData FTK Imager 3.0.0.1443, PMDump 1.2) operate in the system’s user mode, which makes them susceptible to anti-dumping activities performed by active debugging protection systems such as Protect GameGuard. An internal comparison between Belkasoft Live RAM Capturer and latest versions of competing RAM acquisition tools demonstrated the ability of Belkasoft Live RAM Capturer to acquire an image of a protected memory set while the other tools returned an empty area (FTK Imager) or random data (PMDump).Testing methodology: we launched Karos, a computer game protected with nProtect GameGuard. Then we performed an active chat session, and tried acquiring the complete memory dump of the system with all three memory dumping tools. We then analyzed the memory set belonging to the protected game.

Rob Lee Harbinger(2008) developedSIFT (SANS investigative forensic toolkit). The workstation is freely available as Ubuntu 14.04. SIFT is a suite of forensic tools you need and one of the most popular open source incident response platform .The SIFT Workstation is a group of free open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings. It can match any current incident response and forensic tool suite. SIFT demonstrates that advanced incident response capabilities and deep dive digital forensic techniques to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated Rob Lee and his team created and continually update the SIFT Workstation. It's successfully used for incident response and digital forensics and is available to the community as a public service. With over 100,000 downloads to date, the SIFT continues to be the most popular open-source incident-response and digital forensic offering next to commercial source solutions. The SIFT Workstation has quickly become my "go to" tool when conducting an exam. The powerful open source forensic tools in the kit on top of the versatile and stable Linux operating system make for quick access to most everything I need to conduct a thorough analysis of a computer system," said Ken Pryor, GCFA Robinson, IL Police Department.

PALADIN forensic suite – the world’s most famous Linux forensic suite is a modified Linux distro based on Ubuntu available in 32 and 64 bit .PALADIN is a modified “live” Linux distribution based on Ubuntu that simplifies various forensics tasks in a forensically sound manner via the PALADIN Toolbox. PALADIN is available in 64-bit and 32-bit versions. PALADIN has become the World’s #1 Forensic Suite used by thousands of digital forensic examiners from Law Enforcement, Military, Federal, State and Corporate agencies.P222ALADIN

– Version 7 includes Autopsy. Autopsy is a FULL Featured GUI Forensic Suite with all the features that you would expect in a forensic tool. Autopsy even contains advanced features not found in forensic suites that cost thousands. Autopsy combined with PALADIN allows a user to conduct a forensic exam from beginning to end – triage to reporting and everything in-between on Mac, Windows, Linux and Android.

Digital Forensic (2008) created CAINE (Computer Aided Investigative Environment). Currently the project manager is Nanni Bassetti (Bari-Italy). CAINE offers a complete forensic environment that is recognized to integrate existing software tools as software modules and to provide a friendly graphical interface. The main design objectives that CAINE aims to guarantee are, An interoperable environment that supports the digital investigator during the phases of the digital investigation, A user –friendly graphical interface. User-friendly tools. Caine represents fully the spirit of the Open source philosophy, because the project is completely open, everyone could take on the legacy of the previous developer or project manager. The distro is open source, the Windows side is freeware and, the last but not least, the distro is installable.

X-Ways Forensics "Flagship product" is an advanced platform for digital forensics examiners. It runs on all available version of Windows. It claims to not be very resource hungry and to work efficiently. If we talk about the features, find the key features in the list below: Disk imaging and cloning , Ability to read file system structures inside various image files, It supports most of the file systems including
FAT12, FAT16, FAT32, exFAT, TFAT, NTFS,Ext2, Ext3, Ext4, Next3®,
CDFS/ISO9660/Joliet, UDF Automatic detection of deleted or lost hard disk partition ,Various data recovery techniques and powerful file carving Bulk hash calculation, Viewing and editing binary data structures using templates, Easy detection of and access NTFS ADS, Well maintained file header ,Automated activity logging ,Data authenticity, Complete case management Memory and RAM analysis, Gallery view for pictures ,Internal viewer for Windows registry file, Automated registry report , Extracts metadata from various file types ,Ability to extract emails from various available email clients.

Shawn Mccreght the founder of Guidance software EnCase (1998) “EnCase is another popular multi-purpose forensic platform with many nice tools for several areas of the digital forensic process. This tool can rapidly gather data from various devices and unearth potential evidence. It also produces a report based on the evidence. EnCase is traditionally used in forensics to recover evidence from seized hard drives. EnCase allows the investigator to conduct in depth analysis of user files t collect evidence such as documents, pictures, internet history and Windows Registry information. The company also offers EnCase training and certification Data recovered by EnCase has been used in various court systems, such as in the cases of the BTK Killer and the murder of Danielle van Dam. Additional EnCase forensic work was documented in other cases such as the evidence provided for the Casey Anthony, Unabomber, and Mucko (Wakefield Massacre) cases.

X,Wayn (2019) developed the software WinHex “is a commercialdisk editorand universalhexadecimaleditor (hex eitor) used fordata recoveryanddigital forensics. WinHex, made by X-Ways Software Technology AG ofGermany, is a software application that can be used as an advanced hex editor, a tool for data analysis, editing, and recovery, a data wiping tool, and a forensics tool used for evidence gathering. Customers using WinHex include academics and forensics practitioners he Oak Ridge National Laboratory, Hewlett Packard, National Semiconductor, law enforcement agencies, and other companies with data recovery and protection needs. WinHex, compatible with Windows.

XPthroughWindows 10 offers the ability to: Read and directly edit hard drives (FAT and NTFS), floppy disks, CD-ROMs, DVDs, Compact Flash cards, and other media .Read and directly edit RAM ,Interpret 20 data types ,Edit partition tables, boot sectors, and other data structures using templates, Join and split files Analyze and compare files, Search and replace, Clone and image drives, Recover data, Encrypt files (128-bit strength),Create hashes and checksums and Wipe drives Forensics features with a Specialist license, include the ability to, Gather free and slack space ,Search for text based on keywords ,Create tab-delimited tables of drive contents. These tables can be imported into a spreadsheet such as Microsoft Excel and sorted.

The Naval Postgraduates School, an agency of the U.S Department of Navy (2012) developed Bulk extractor. It is a computer forensics tool that scans a disk image, file, or directory of files and extracts information such as credit card numbers, domains, e-mail addresses, URLs, and ZIP files. The extracted information is output to a series of text files (which can be reviewed manually or analyzed using other forensics tools or scripts).Tip: Within the output text files you will find entries for data that resemble a credit card number, e-mail address, domain name, etc. You will also see a decimal value in the first column of the text file that, when converted to hex, can be used as the pointer on disk where the entry was found (i.e. if you were analyzing the disk manually using a hex editor for example, you would jump to this hexadecimal value to view the data).Bulk extractor comes as a command-line tool or a GUI tool. In the example above I set the bulk extractor tool to extract information from a forensics image I took earlier and output the results to a folder called “BE Output”. The results can then be viewed in the Bulk Extractor Viewer and the output text files mentioned above. Key features are ,Processes different parts of the disk in parallel, Automatically detects, decompresses, and reprocesses compressed data ,Extracts critical information such as credit card details and email addresses from digital data and Can be used to process information across most digital media.

# CHAPTER III

## AIM AND OBJECTIVES

**AIM:**

To study of AccessData_FTK_Imager_4.2.1 for password cracking and dumpIt version 3.2 for capturing of raw files.

**OBJECTIVES:**

- To ensure the software are user friendly.
- To extract there artifacts from the image.
- To identify the role of free software's in capturing of  passwords.
- Forensic significance of this software.

# CHAPTER IV

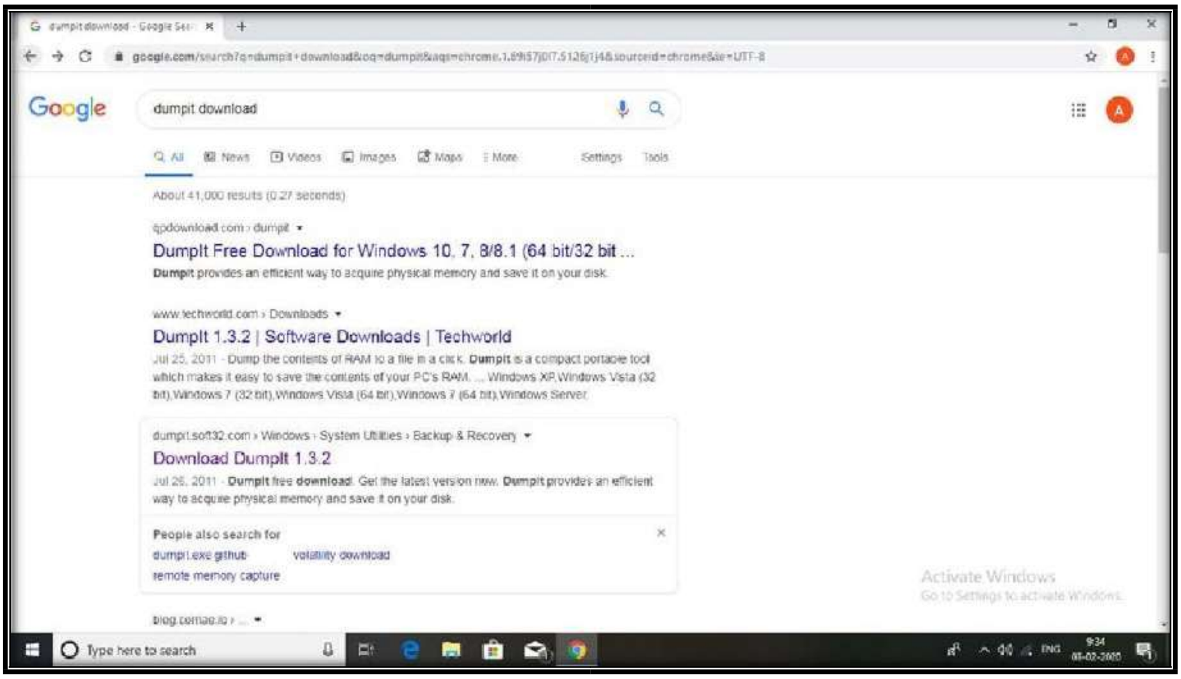
# MATERIALS AND METHODOLOGY

## MATERIALS:

- Personnel computer(PC)
- AccessData_FTK_Imager_4.2.1
- dumpIt version 3.2
- Raw Live Image Captured (05 collected sample)

## METHODOLOGY:

### Step I– Install dumpIt version 1.3.2


dumpit download - Google Sea
google.com/search?q=dumpit+download&oq=dumpit&aqs=chrome.1.69i57j0l7.5126j1j4&sourceid=chrome&ie=UTF-8
Google
All
News
Videos
Images
Maps
More
Settings
Tools
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
9:34
03-02-2020

dumpit download

About 41,000 results (0.27 seconds)

qpdownload.com › dumpit ▾

DumpIt Free Download for Windows 10, 7, 8/8.1 (64 bit/32 bit ...

**Dumpit** provides an efficient way to acquire physical memory and save it on your disk.

www.techworld.com › Downloads ▾

DumpIt 1.3.2 | Software Downloads | Techworld

Jul 25, 2011 - Dump the contents of RAM to a file in a click. **Dumpit** is a compact portable tool which makes it easy to save the contents of your PC's RAM. ... Windows XP,Windows Vista (32 bit),Windows 7 (32 bit),Windows Vista (64 bit),Windows 7 (64 bit),Windows Server

dumpit.soft32.com › Windows › System Utilities › Backup & Recovery ▾

Download DumpIt 1.3.2

Jul 26, 2011 - **DumpIt free download**. Get the latest version now. **Dumpit** provides an efficient way to acquire physical memory and save it on your disk.

People also search for

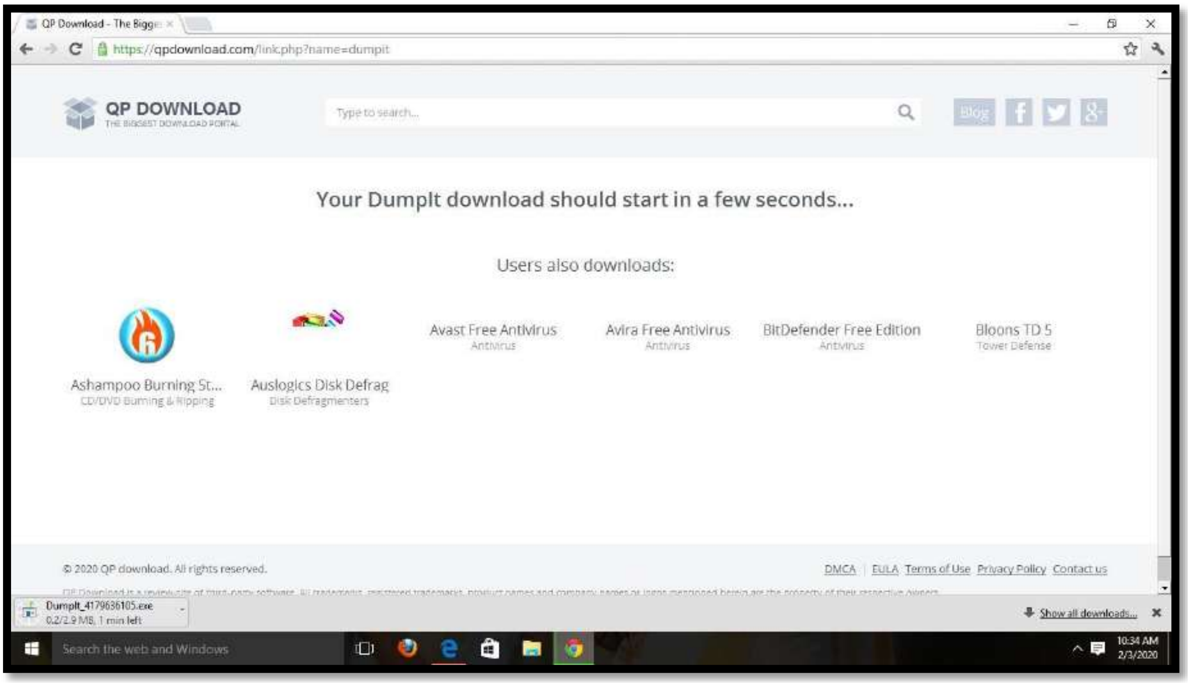
dumpit.exe github

volatility download

remote memory capture

blog.comae.io › ... ▾

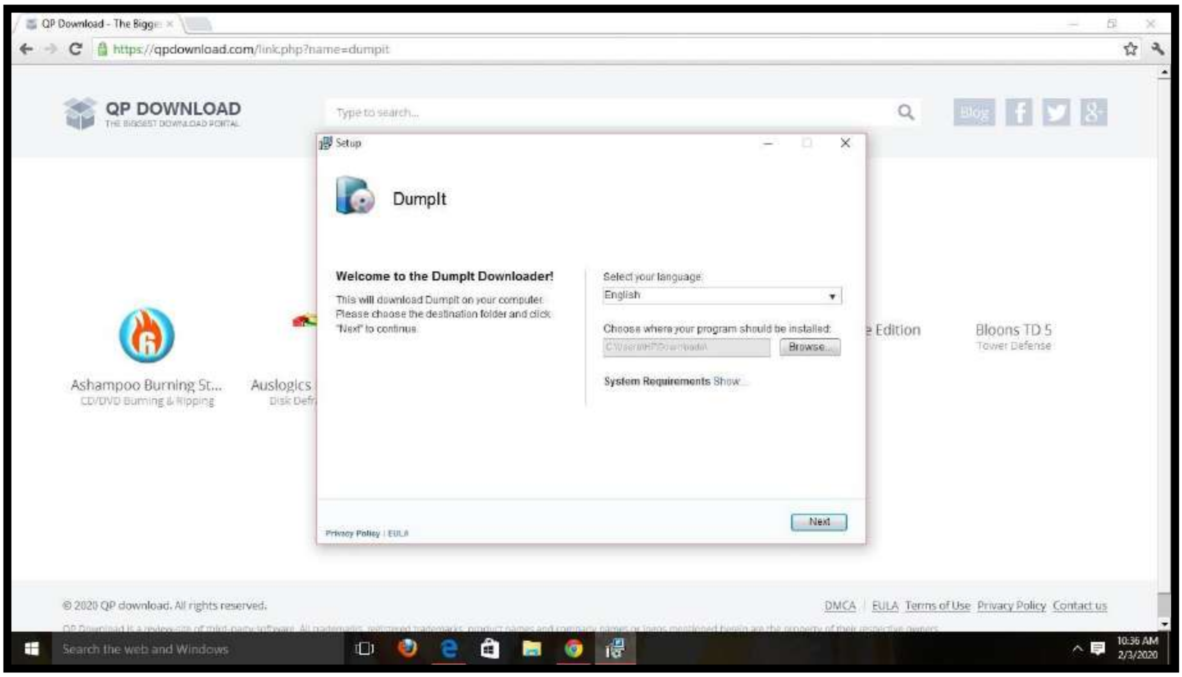
**Fig I.i Browsing of the DumpIt Version 1.3.2**



QP Download - The Bigge
https://qpdownload.com/link.php?name=dumpit
QP DOWNLOAD
THE BIGGEST DOWNLOAD PORTAL
Type to search...
Blog

Your DumpIt download should start in a few seconds...

**Fig I.ii Downloading of the DumpIt Version 1.3.2**



QP Download - The Bigge
https://qpdownload.com/link.php?name=dumpit
QP DOWNLOAD
THE BIGGEST DOWNLOAD PORTAL
Type to search...
Blog
Setup
DumpIt

Welcome to the DumpIt Downloader!

This will download DumpIt on your computer. Please choose the destination folder and click "Next" to continue.

Select your language: English

Choose where your program should be installed: C:\Users\HP\Downloads\

**Fig I.iii Starting of DumpIt Installation**

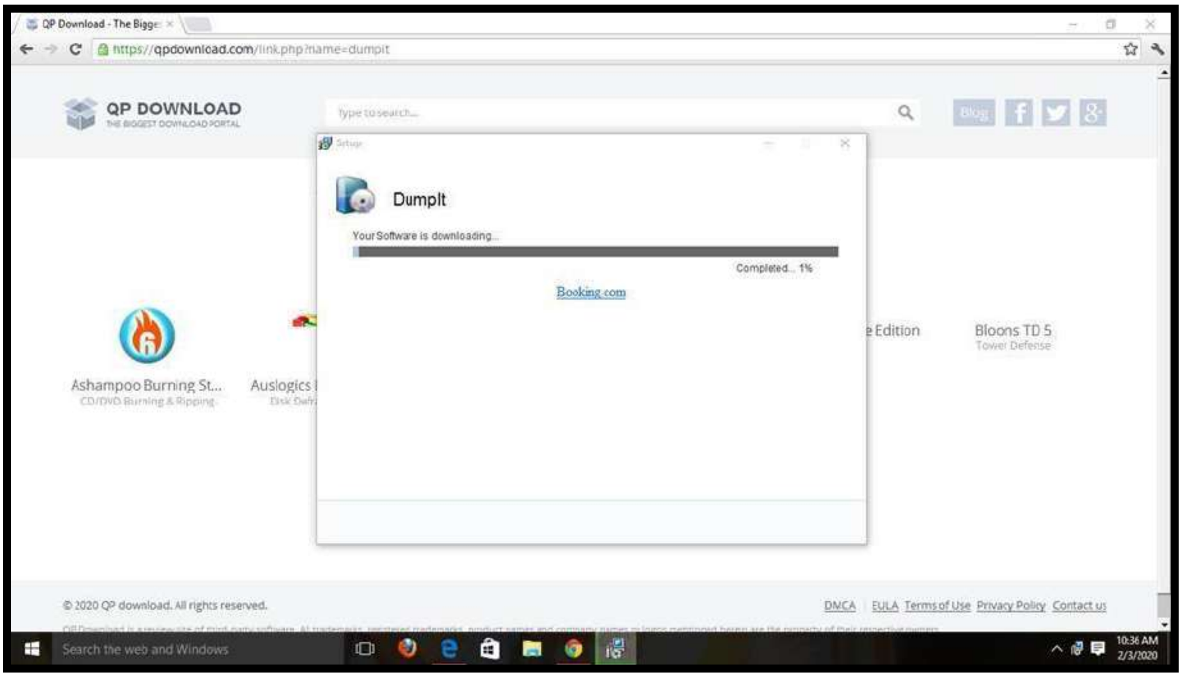
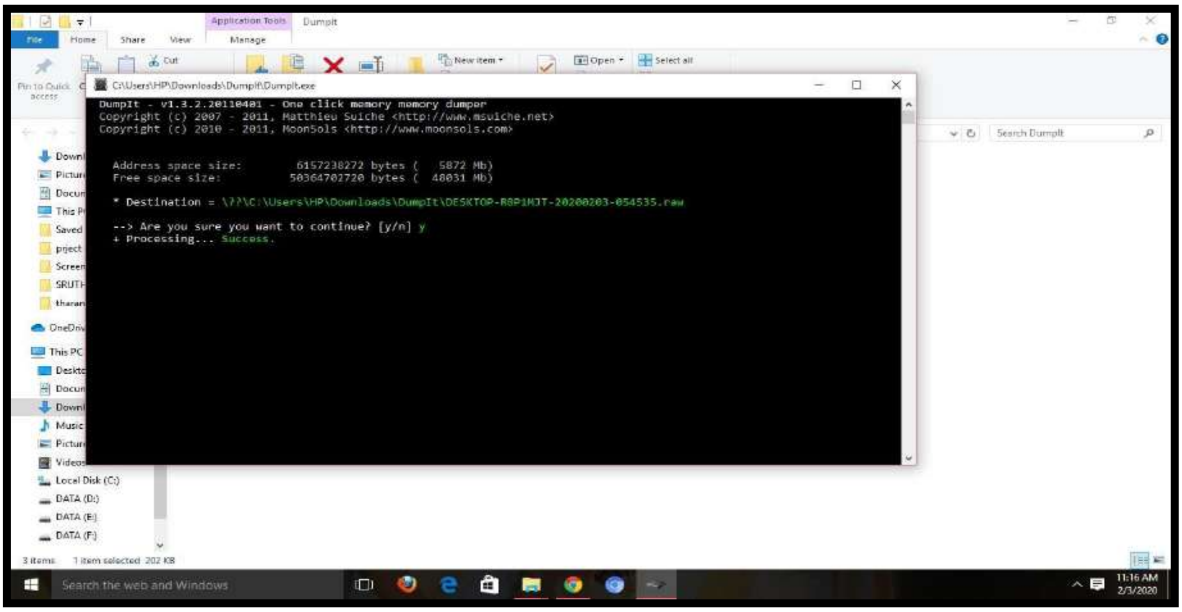


Fig I.iv Installation of dumpIt

**Step II- Extract dumpIt files and let it run in command prompt**



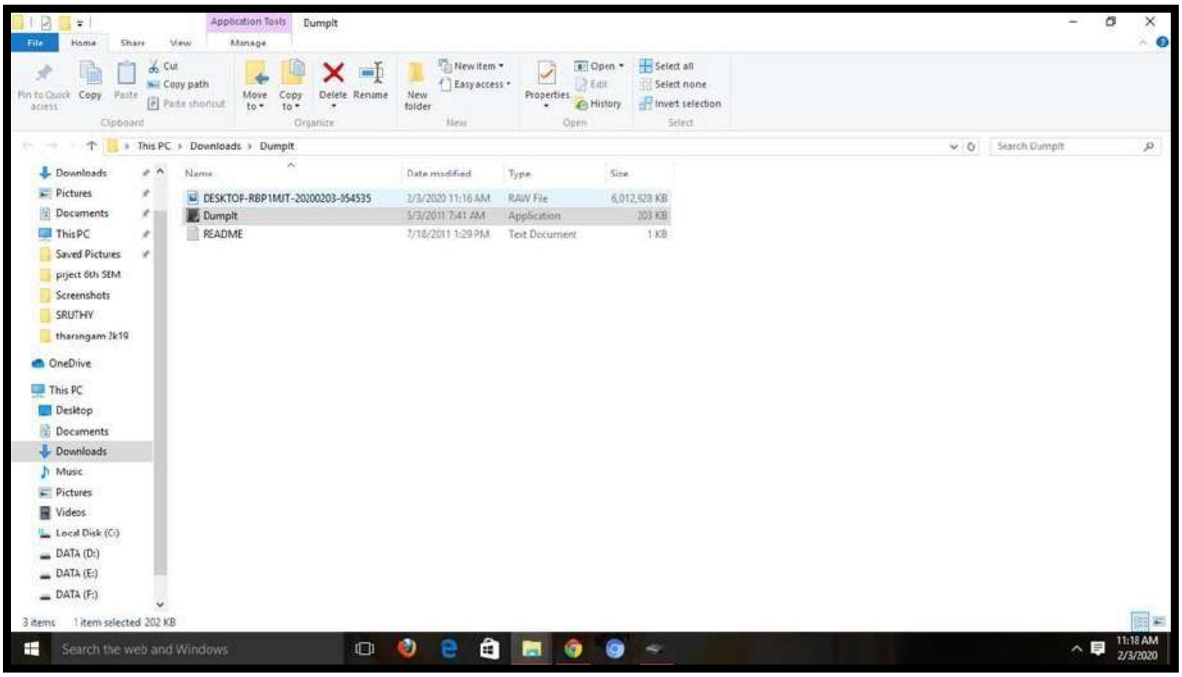
```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


  Address space size:        6157238272 bytes (   5872 Mb)
  Free space size:          50364702720 bytes (  48031 Mb)

  * Destination = \??\C:\Users\HP\Downloads\DumpIt\DESKTOP-R8P1MJT-20200203-054535.raw

  --> Are you sure you want to continue? [y/n] y
  + Processing... Success.
```

Fig II.i Successfully completed the raw image capturing



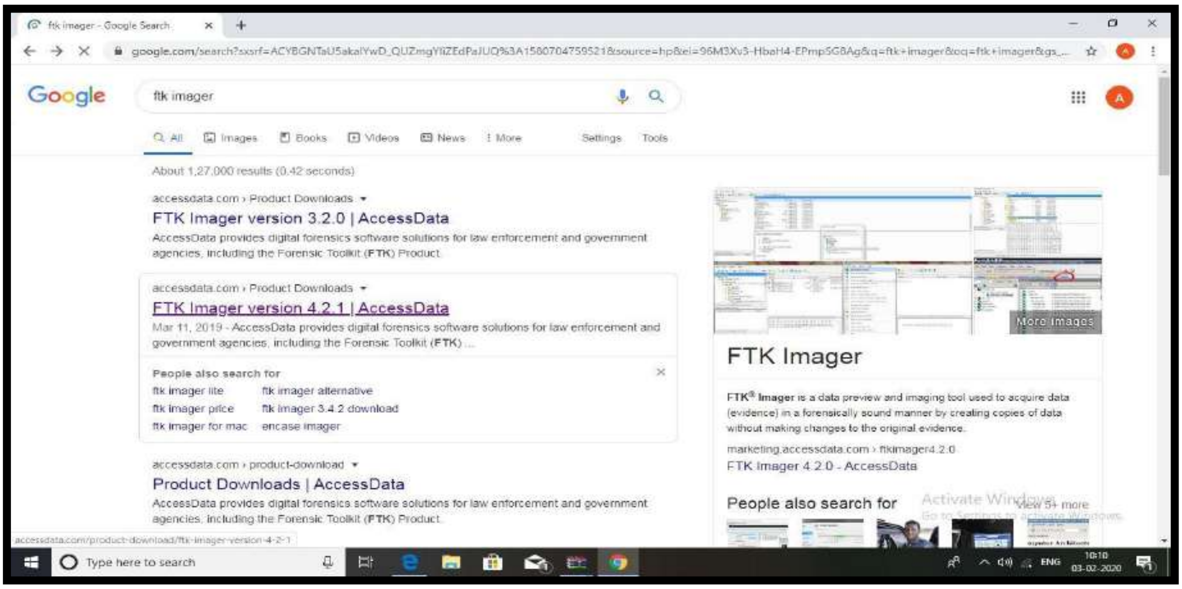
This PC › Downloads › DumpIt

| Name | Date modified | Type | Size |
|---|---|---|---|
| DESKTOP-RBP1MJT-20200203-054535 | 2/3/2020 11:16 AM | RAW File | 6,012,928 KB |
| DumpIt | 5/3/2011 7:41 AM | Application | 203 KB |
| README | 7/18/2011 1:29 PM | Text Document | 1 KB |

3 items 1 item selected 202 KB

**Fig II. ii Generated raw file**

## Step III -Install AccessData_FTK_Imager



google.com/search?sxsrf=ACYBGNTaU5akalYwD_QUZmgYIiZEdPaJUQ%3A1580704759521&source=hp&ei=96M3Xv5-HbaH4-EPmp5G8Ag&q=ftk+imager&oq=ftk+imager&gs_...

ftk imager

About 1,27,000 results (0.42 seconds)

accessdata.com › Product Downloads

FTK Imager version 3.2.0 | AccessData

AccessData provides digital forensics software solutions for law enforcement and government agencies, including the Forensic Toolkit (FTK) Product

accessdata.com › Product Downloads

FTK Imager version 4.2.1 | AccessData

Mar 11, 2019 - AccessData provides digital forensics software solutions for law enforcement and government agencies, including the Forensic Toolkit (FTK) ...

People also search for

ftk imager lite ftk imager alternative
ftk imager price ftk imager 3.4.2 download
ftk imager for mac encase imager

accessdata.com › product-download

Product Downloads | AccessData

AccessData provides digital forensics software solutions for law enforcement and government agencies, including the Forensic Toolkit (FTK) Product

accessdata.com/product-download/ftk-imager-version-4-2-1

FTK Imager

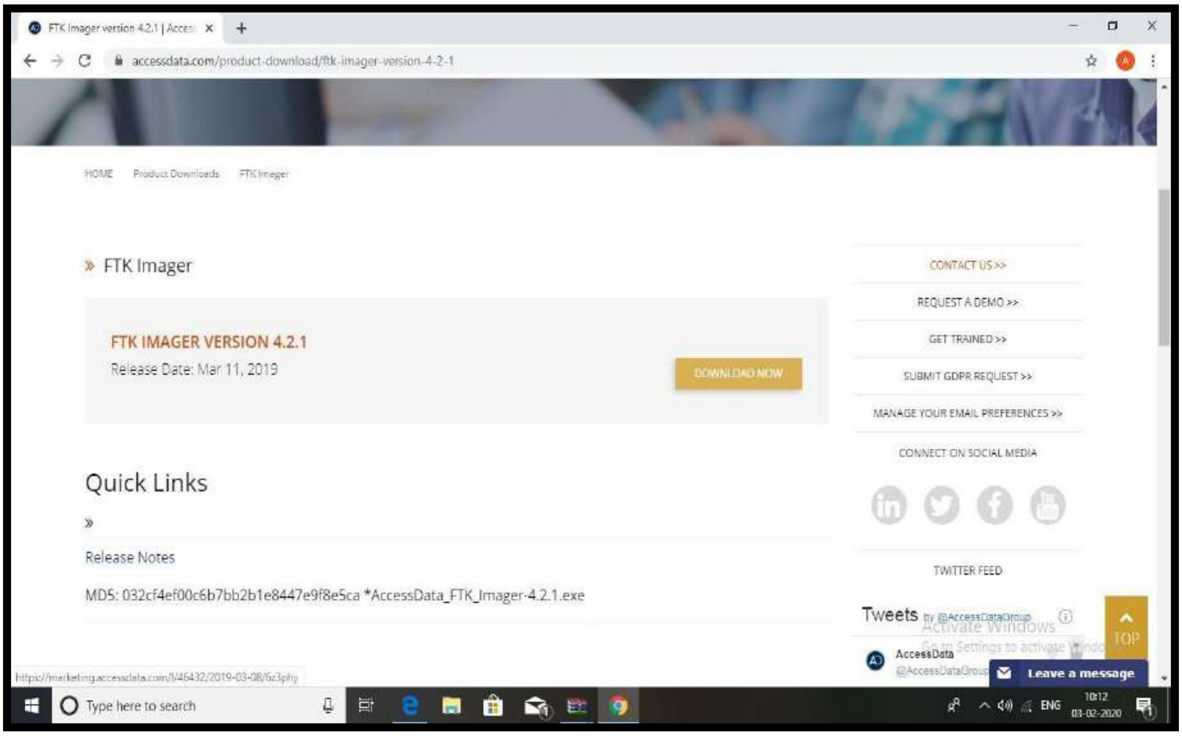
FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence.

marketing.accessdata.com › ftkimager4.2.0

FTK Imager 4.2.0 - AccessData

People also search for

**Fig III.i Browsing of AccessData_FTK_Imager version 4.2.1**



FTK Imager version 4.2.1 | Access
accessdata.com/product-download/ftk-imager-version-4-2-1

HOME Product Downloads FTK Imager

» FTK Imager

FTK IMAGER VERSION 4.2.1

Release Date: Mar 11, 2019

Quick Links

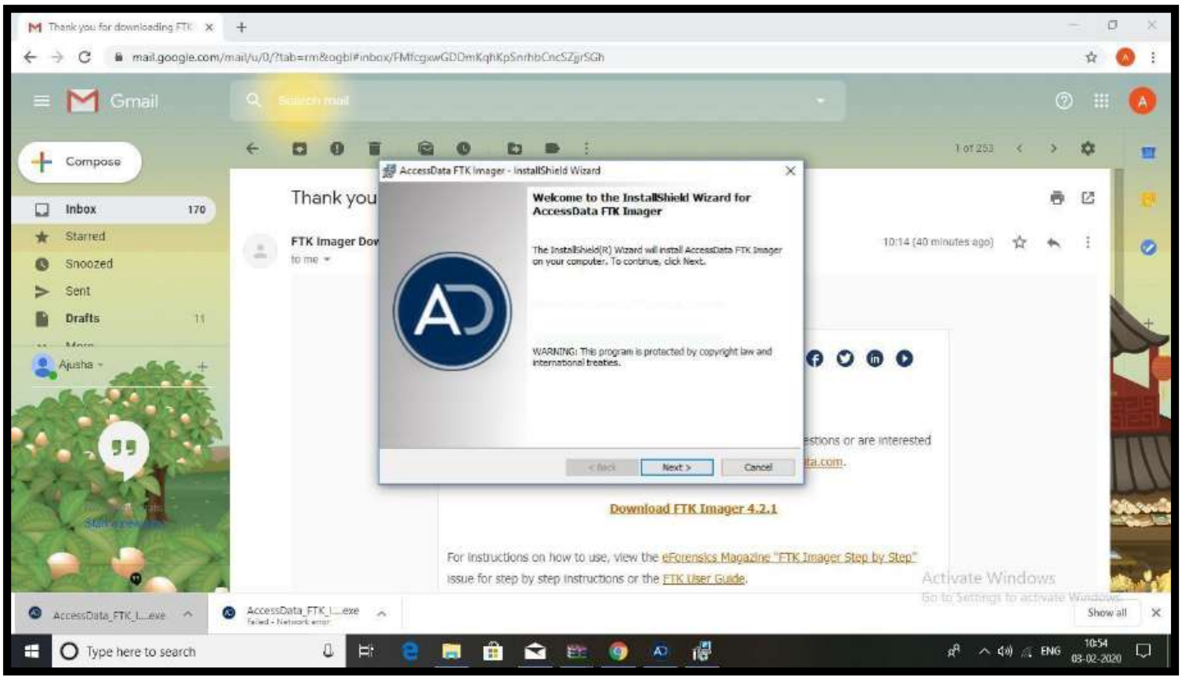
»

Release Notes

MD5: 032cf4ef00c6b7bb2b1e8447e9f8e5ca *AccessData_FTK_Imager-4.2.1.exe

CONTACT US >>
REQUEST A DEMO >>
GET TRAINED >>
SUBMIT GDPR REQUEST >>
MANAGE YOUR EMAIL PREFERENCES >>
CONNECT ON SOCIAL MEDIA
TWITTER FEED
Tweets by @AccessDataGroup
AccessData
@AccessDataGroup
TOP
Leave a message
Activate Windows
Go to Settings to activate Windows.
https://marketing.accessdata.com/l/46432/2019-03-08/6z3phy
Type here to search
ENG
10:12
03-02-2020

**Fig III.ii Downloading of AccessData_FTK_Imager version 4.2.1**



Thank you for downloading FTK
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgxwGDDmKqhKpSnrhbCncSZjrSGh
Gmail
Search mail
Compose
Inbox 170
Starred
Snoozed
Sent
Drafts 11
More
Ajusha
1 of 253

Thank you

FTK Imager Dow
to me

10:14 (40 minutes ago)

AccessData FTK Imager - InstallShield Wizard

**Welcome to the InstallShield Wizard for AccessData FTK Imager**

The InstallShield(R) Wizard will install AccessData FTK Imager on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

estions or are interested

ta.com.

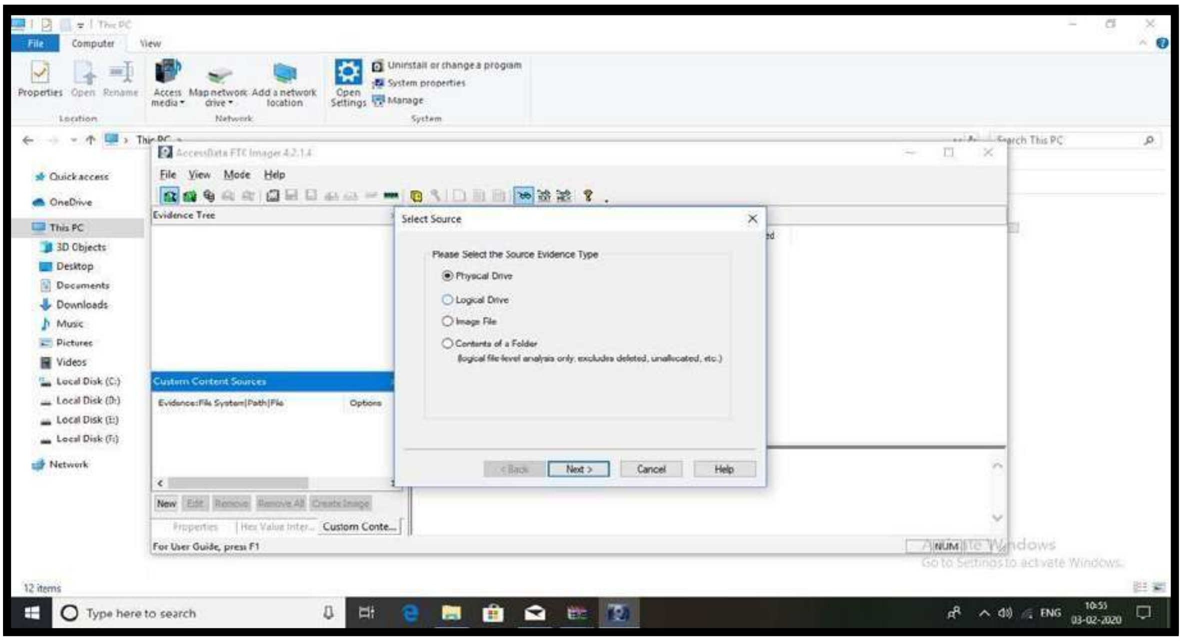
Download FTK Imager 4.2.1

For instructions on how to use, view the eForensics Magazine "FTK Imager Step by Step" issue for step by step instructions or the FTK User Guide.

**Fig III.iii Open your respective mail click on the link for installing AccessData_FTK_Imager version 4.2.1**

**Step IV- Click on add evidence**

## Step V- Capturing of Password



Select Source

Please Select the Source Evidence Type

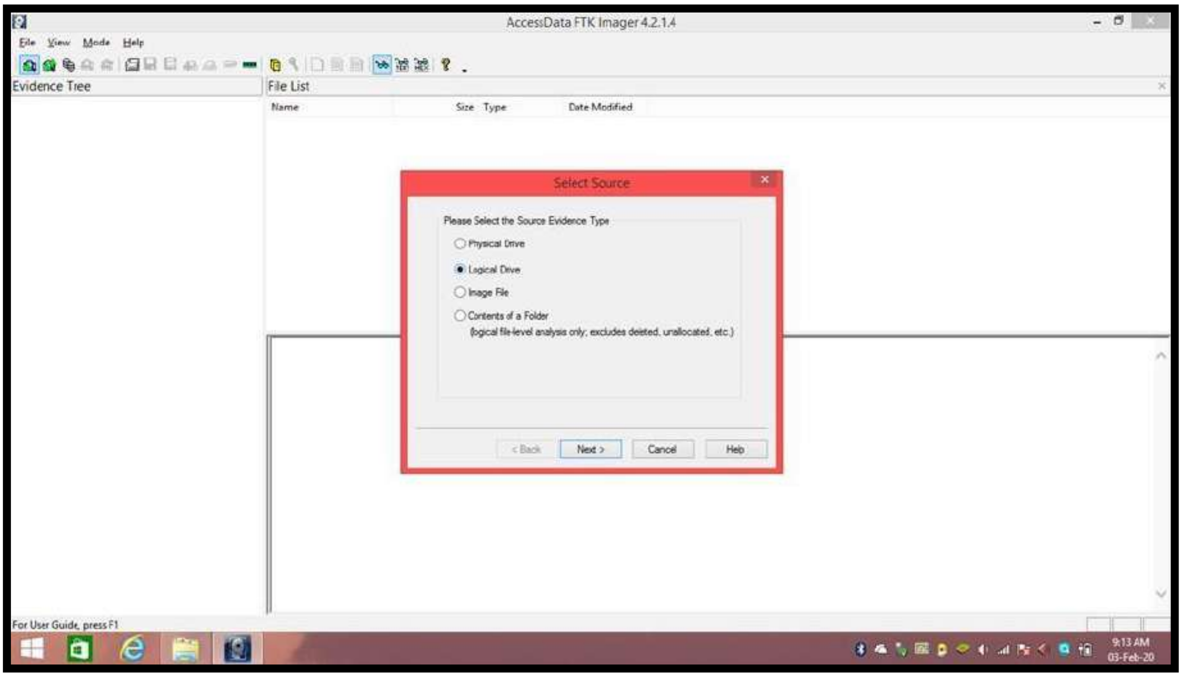
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Fig V.i Click on the physical drive (if the cracking password of the system itself)



Select Source

Please Select the Source Evidence Type

○ Physical Drive

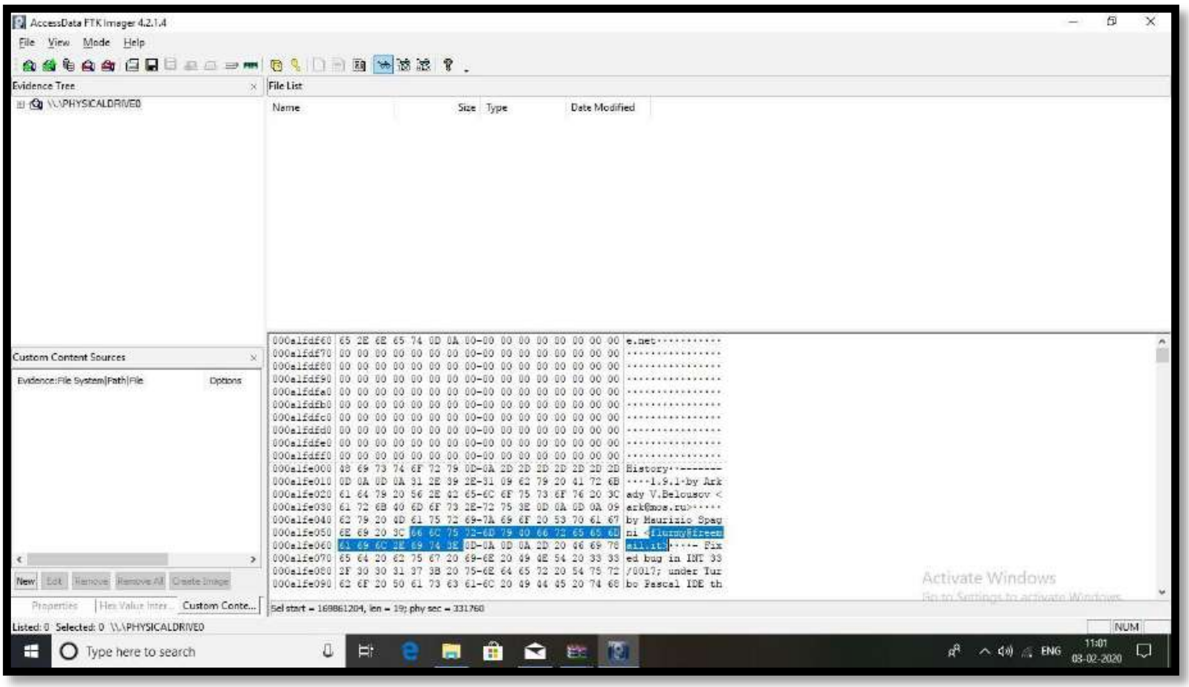
● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Fig V.ii Click on the logical drive (if the cracking password from other computers raw Image)

## Step VI-Captured image



AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
NUM
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
11:01
03-02-2020

```
000a1fdf60 65 2E 6E 65 74 0D 0A 00-00 00 00 00 00 00 00 00 e.net···········
000a1fdf70 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdf80 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdf90 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdfa0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdfb0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdfc0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdfd0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdfe0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fdff0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
000a1fe000 48 69 73 74 6F 72 79 0D-0A 2D 2D 2D 2D 2D 2D 2D History··-------
000a1fe010 0D 0A 0D 0A 31 2E 39 2E-31 09 62 79 20 41 72 6B ····1.9.1·by Ark
000a1fe020 61 64 79 20 56 2E 42 65-6C 6F 75 73 6F 76 20 3C ady V.Belousov <
000a1fe030 61 72 6B 40 6D 6F 73 2E-72 75 3E 0D 0A 0D 0A 09 ark@mos.ru>·····
000a1fe040 62 79 20 4D 61 75 72 69-7A 69 6F 20 53 70 61 67 by Maurizio Spag
000a1fe050 6E 69 20 3C 66 6C 75 72-6D 79 40 66 72 65 65 6D ni <flurmy@freem
000a1fe060 61 69 6C 2E 69 74 3E 0D-0A 0D 0A 2D 20 46 69 78 ail.it>····- Fix
000a1fe070 65 64 20 62 75 67 20 69-6E 20 49 4E 54 20 33 33 ed bug in INT 33
000a1fe080 2F 30 30 31 37 3B 20 75-6E 64 65 72 20 54 75 72 /0017; under Tur
000a1fe090 62 6F 20 50 61 73 63 61-6C 20 49 44 45 20 74 68 bo Pascal IDE th
```

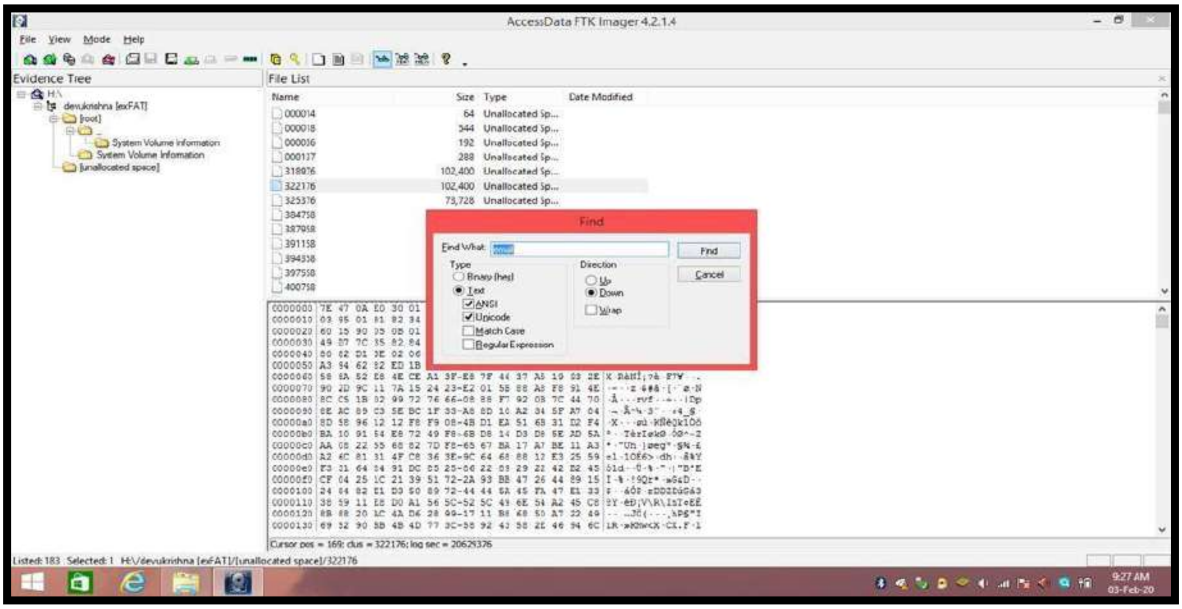
Sel start = 169861204, len = 19; phy sec = 331760

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig VI.i Captured image

## Step VII- Click ctrl+f

## Step VIII- By using various strings like email & password try to cracking passwords and mail id



| Name | Size | Type | Date Modified |
|---|---|---|---|
| 000014 | 64 | Unallocated Sp... | |
| 000018 | 544 | Unallocated Sp... | |
| 000036 | 192 | Unallocated Sp... | |
| 000137 | 288 | Unallocated Sp... | |
| 318976 | 102,400 | Unallocated Sp... | |
| 322176 | 102,400 | Unallocated Sp... | |
| 325376 | 73,728 | Unallocated Sp... | |
| 384758 | | | |
| 387958 | | | |
| 391158 | | | |
| 394358 | | | |
| 397558 | | | |
| 400758 | | | |

Find

Find What: email

Type
○ Binary (hex)
● Text
☑ ANSI
☑ Unicode
□ Match Case
□ Regular Expression

Direction
○ Up
● Down
□ Wrap

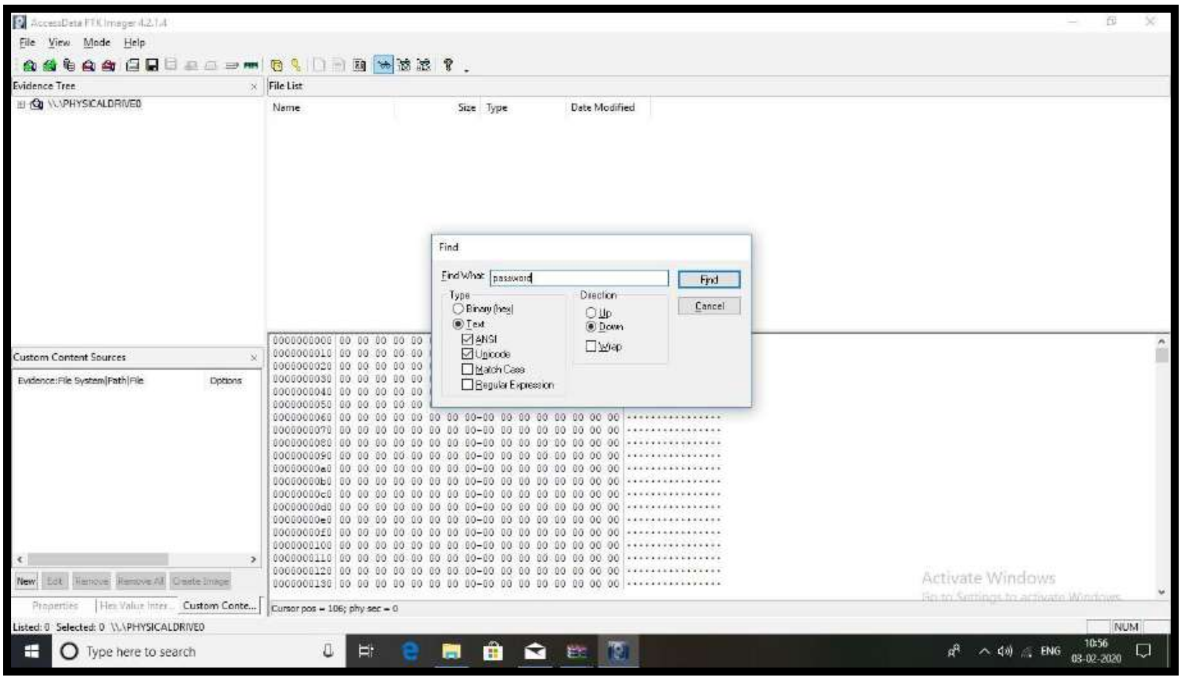
Find Cancel

```
0000000 7E 47 0A E0 30 01
0000010 03 95 01 81 82 34
0000020 60 15 90 05 0B 01
0000030 49 87 7C 35 82 84
0000040 80 62 D1 3E 02 06
0000050 A3 94 62 82 ED 1B
0000060 58 8A 52 E8 4E CE A1 3F-E8 7F 44 37 A5 10 03 2E X RAN‌Î¡?è F7¥ ·.
0000070 90 2D 9C 11 7A 15 24 23-E2 01 5B 88 A8 F8 91 4E ·-··z·$#â·[·¨ø·N
0000080 8C C5 1B 02 99 72 76 66-08 88 F7 92 08 7C 44 70 ·Å···rvf··÷··|Dp
0000090 8E AC 89 C3 5E BC 1F 33-A8 8D 10 A2 34 5F A7 04 ·¬·Ã^¼·3¨··¢4_§·
00000a0 8D 58 96 12 12 F8 F9 08-4B D1 EA 51 6B 31 D2 F4 ·X···øù·KÑêQk1Òô
00000b0 BA 10 91 54 E8 72 49 F8-6B D8 14 D3 D8 5E AD 5A º··TèrIøkØ·ÓØ^-Z
00000c0 AA 08 22 55 68 82 7D F8-65 67 BA 17 A7 BE 11 A3 ª·"Uh·}øeg º·§¾·£
00000d0 A2 4C 81 31 4F C8 36 3E-9C 64 68 88 12 E3 25 59 ¢L·1OÈ6>·dh··ã%Y
00000e0 F3 31 64 84 91 DC D5 25-66 22 08 29 22 42 D2 45 ó1d··ÜÕ%f"·)"BÒE
00000f0 CF 04 25 1C 21 39 51 72-2A 93 BB 47 26 44 89 15 Ï·%·!9Qr*·»G&D··
0000100 24 84 82 E1 D3 50 89 72-44 44 5A 45 FA 47 E1 33 $··áÓP·rDDZEúGá3
0000110 38 59 11 E8 D0 A1 56 5C-52 5C 49 6E 54 A2 45 C8 8Y·èÐ¡V\R\InT¢EÈ
0000120 8B 88 20 1C 4A D6 28 99-17 11 B8 68 50 A7 22 49 ·· ·JÖ(···¸hP§"I
0000130 69 52 90 5B 4B 4D 77 3C-58 92 43 58 2E 46 94 6C iR·[KMw<X·CX.F·l
```

Cursor pos = 169; clus = 322176; log sec = 20629376

Listed: 183 Selected: 1 H:\devukrishna [exFAT]/[unallocated space]/322176

Fig VIII.i while entering the string as email


AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Find
Find Cancel
Activate Windows
Go to Settings to activate Windows.
NUM
Type here to search
ENG
10:56
03-02-2020

Find What: password

Type
○ Binary (hex)
● Text
☑ ANSI
☑ Unicode
□ Match Case
□ Regular Expression

Direction
○ Up
● Down
□ Wrap

```
0000000060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
00000000f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
0000000130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
```

Cursor pos = 106; phy sec = 0

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

**Fig VIII.ii while entering the string as password**

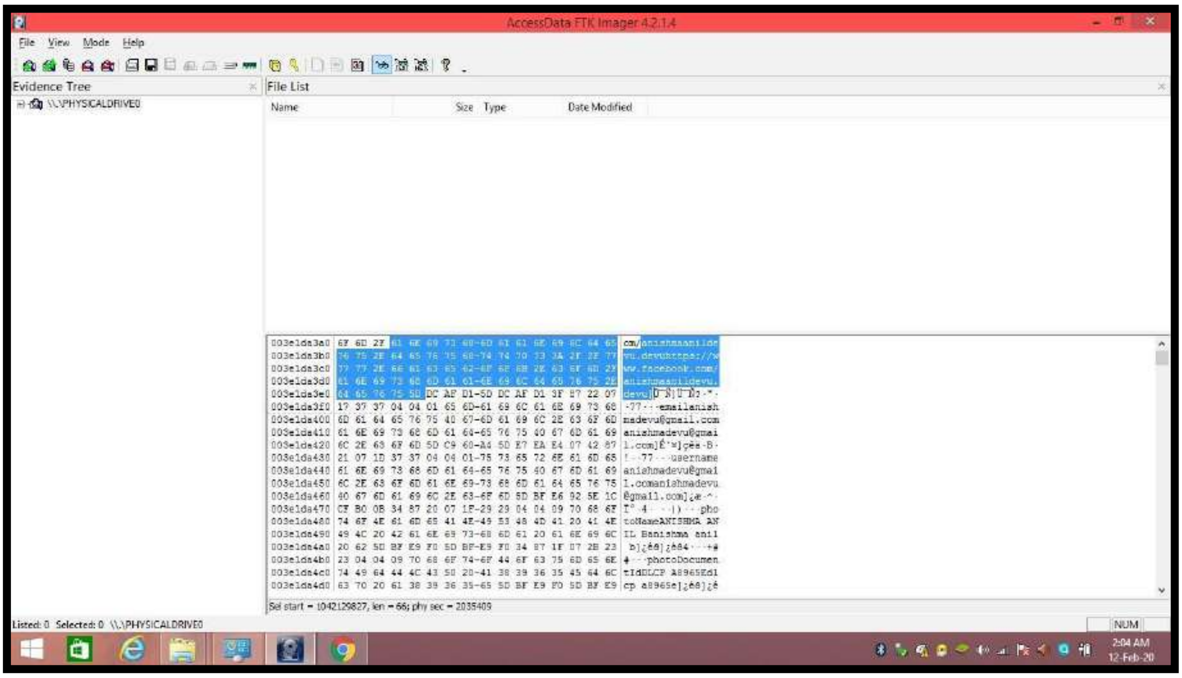
# CHAPTER V

# OBSERVATION AND FINDINGS

## OBSERVATION:

### Sample 1

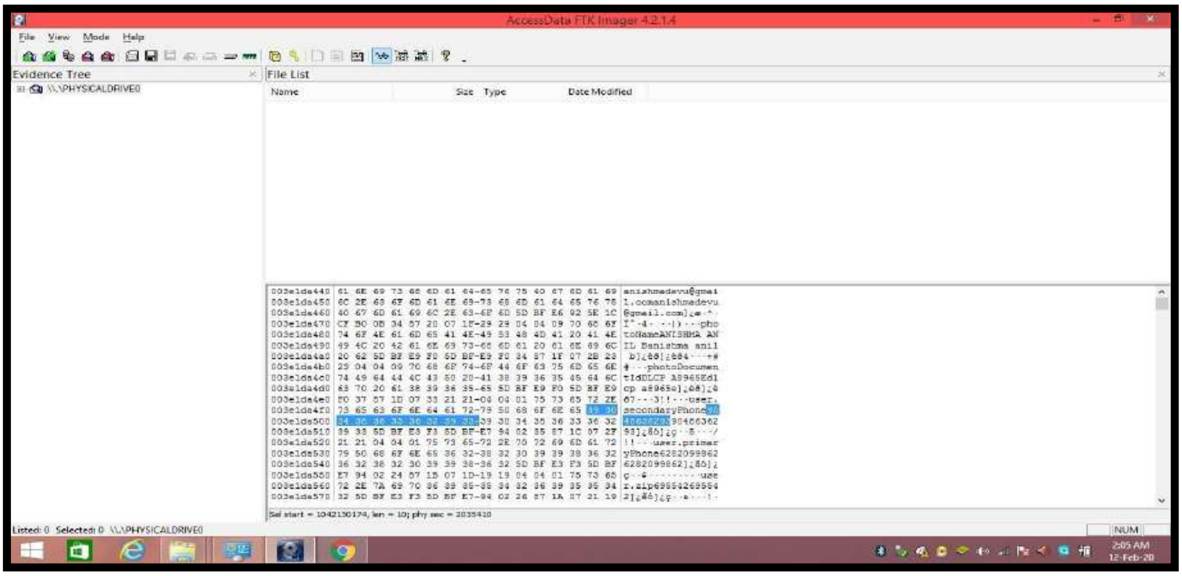
**Observation: Captured Facebook Id and Password**



```
003e1da3a0  6F 6D 2F 61 6E 69 73 68-6D 61 61 6E 69 6C 64 65  om/anishmaanilde
003e1da3b0  76 75 2E 64 65 76 75 68-74 74 70 73 3A 2F 2F 77  vu.devuhttps://w
003e1da3c0  77 77 2E 66 61 63 65 62-6F 6F 6B 2E 63 6F 6D 2F  ww.facebook.com/
003e1da3d0  61 6E 69 73 68 6D 61 61-6E 69 6C 64 65 76 75 2E  anishmaanildevu.
003e1da3e0  64 65 76 75 5D DC AF D1-5D DC AF D1 3F 87 22 07  devu]Ü¯Ñ]Ü¯Ñ?·"·
003e1da3f0  17 37 37 04 04 01 65 6D-61 69 6C 61 6E 69 73 68  ·77···emailanish
003e1da400  6D 61 64 65 76 75 40 67-6D 61 69 6C 2E 63 6F 6D  madevu@gmail.com
003e1da410  61 6E 69 73 68 6D 61 64-65 76 75 40 67 6D 61 69  anishmadevu@gmai
003e1da420  6C 2E 63 6F 6D 5D C9 60-A4 5D E7 EA E4 07 42 87  l.com]É`¤]çêä·B·
003e1da430  21 07 1D 37 37 04 04 01-75 73 65 72 6E 61 6D 65  !··77···username
003e1da440  61 6E 69 73 68 6D 61 64-65 76 75 40 67 6D 61 69  anishmadevu@gmai
003e1da450  6C 2E 63 6F 6D 61 6E 69-73 68 6D 61 64 65 76 75  l.comanishmadevu
003e1da460  40 67 6D 61 69 6C 2E 63-6F 6D 5D BF E6 92 5E 1C  @gmail.com]¿æ·^·
003e1da470  CF B0 0B 34 87 20 07 1F-29 29 04 04 09 70 68 6F  Ï°·4· ··))···pho
003e1da480  74 6F 4E 61 6D 65 41 4E-49 53 48 4D 41 20 41 4E  toNameANISHMA AN
003e1da490  49 4C 20 42 61 6E 69 73-68 6D 61 20 61 6E 69 6C  IL Banishma anil
003e1da4a0  20 62 5D BF E9 F0 5D BF-E9 F0 34 87 1F 07 2B 23   b]¿éð]¿éð4···+#
003e1da4b0  23 04 04 09 70 68 6F 74-6F 44 6F 63 75 6D 65 6E  #···photoDocumen
003e1da4c0  74 49 64 44 4C 43 50 20-41 38 39 36 35 45 64 6C  tIdDLCP A8965Edl
003e1da4d0  63 70 20 61 38 39 36 35-65 5D BF E9 F0 5D BF E9  cp a8965e]¿éð]¿é
Sel start = 1042129827, len = 66; phy sec = 2035409
```

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 1.1 login id of facebook



```
003e1da440  61 6E 69 73 68 6D 61 64-65 76 75 40 67 6D 61 69  anishmadevu@gmai
003e1da450  6C 2E 63 6F 6D 61 6E 69-73 68 6D 61 64 65 76 75  l.comanishmadevu
003e1da460  40 67 6D 61 69 6C 2E 63-6F 6D 5D BF E6 92 5E 1C  @gmail.com]¿æ·^·
003e1da470  CF B0 0B 34 87 20 07 1F-29 29 04 04 09 70 68 6F  Ï°·4· ··))···pho
003e1da480  74 6F 4E 61 6D 65 41 4E-49 53 48 4D 41 20 41 4E  toNameANISHMA AN
003e1da490  49 4C 20 42 61 6E 69 73-68 6D 61 20 61 6E 69 6C  IL Banishma anil
003e1da4a0  20 62 5D BF E9 F0 5D BF-E9 F0 34 87 1F 07 2B 23   b]¿éð]¿éð4···+#
003e1da4b0  23 04 04 09 70 68 6F 74-6F 44 6F 63 75 6D 65 6E  #···photoDocumen
003e1da4c0  74 49 64 44 4C 43 50 20-41 38 39 36 35 45 64 6C  tIdDLCP A8965Edl
003e1da4d0  63 70 20 61 38 39 36 35-65 5D BF E9 F0 5D BF E9  cp a8965e]¿éð]¿é
003e1da4e0  F0 37 87 1D 07 33 21 21-04 04 01 75 73 65 72 2E  ð7···3!!···user.
003e1da4f0  73 65 63 6F 6E 64 61 72-79 50 68 6F 6E 65 39 30  secondaryPhone90
003e1da500  34 36 36 33 36 32 39 33-39 30 34 36 36 33 36 32  4663629390466362
003e1da510  39 33 5D BF E3 F3 5D BF-E7 94 02 35 87 1C 07 2F  93]¿ãó]¿ç··5···/
003e1da520  21 21 04 04 01 75 73 65-72 2E 70 72 69 6D 61 72  !!···user.primar
003e1da530  79 50 68 6F 6E 65 36 32-38 32 30 39 39 38 36 32  yPhone6282099862
003e1da540  36 32 38 32 30 39 39 38-36 32 5D BF E3 F3 5D BF  6282099862]¿ãó]¿
003e1da550  E7 94 02 24 87 1B 07 1D-19 19 04 04 01 75 73 65  ç··$·········use
003e1da560  72 2E 7A 69 70 36 39 35-35 34 32 36 39 35 35 34  r.zip695542695554
003e1da570  32 5D BF E3 F3 5D BF E7-94 02 26 87 1A 87 21 19  2]¿ãó]¿ç··&···!·
Sel start = 1042130174, len = 10; phy sec = 2035410
```

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 1. 2 Password of Facebook

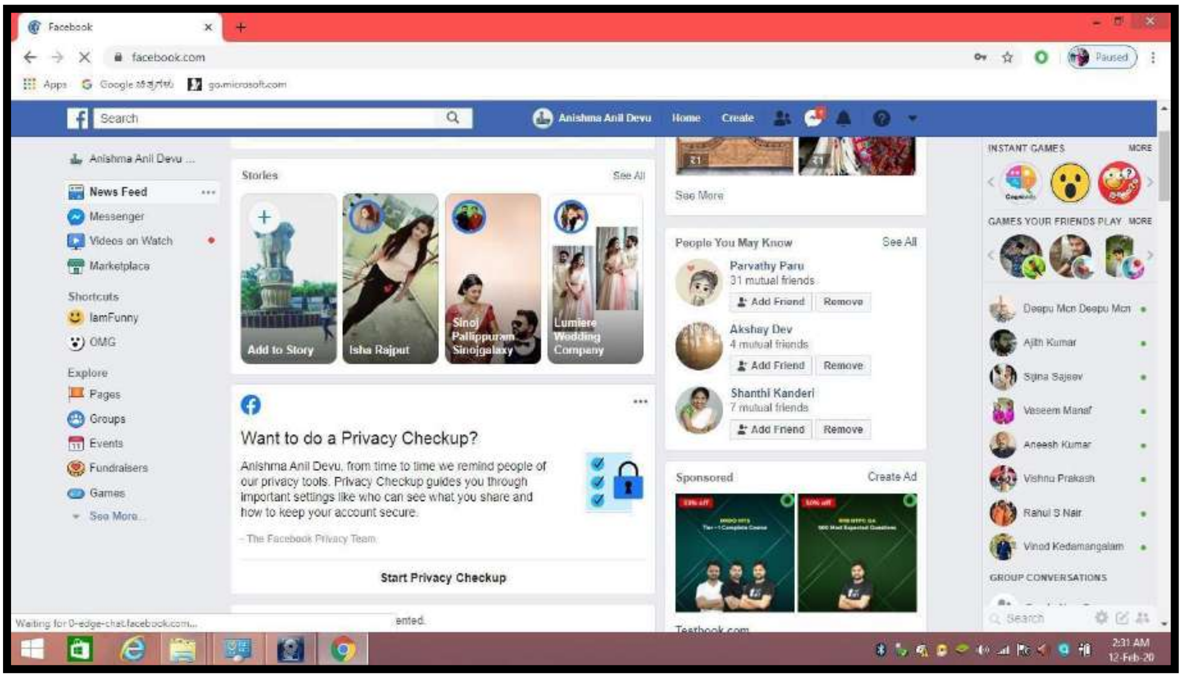
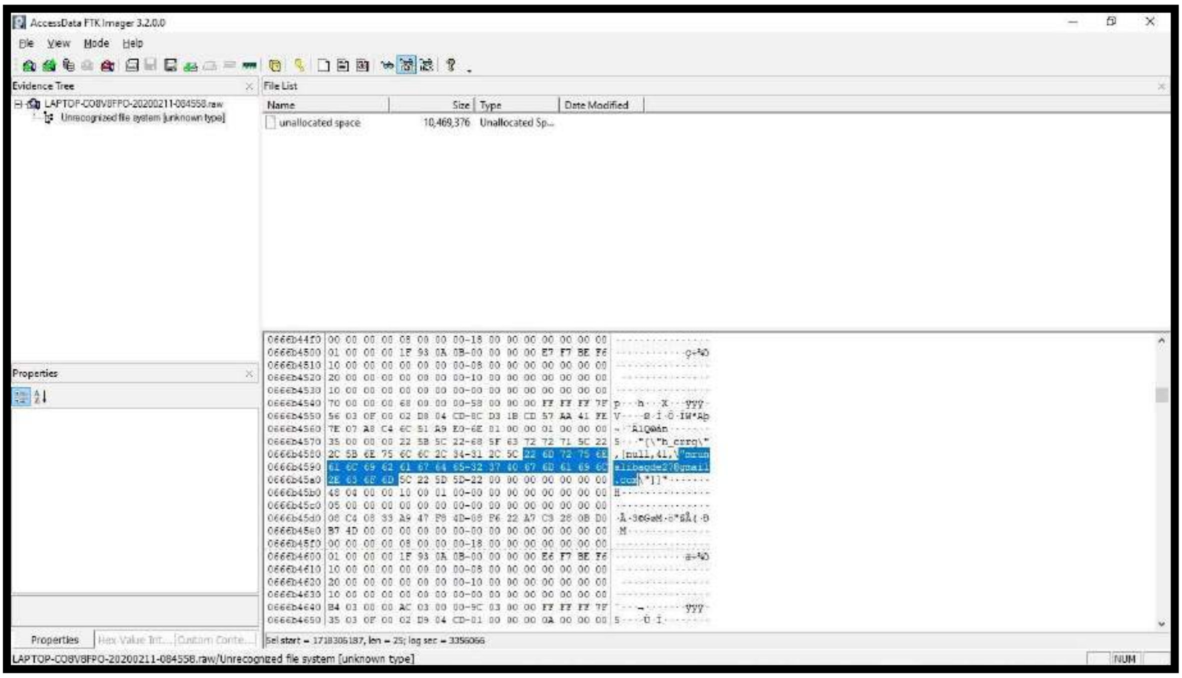


**Fig 1.3 Logged in Page**

## Sample 2

### Observation: Captured Password of Netacad Account


AccessData FTK Imager 3.2.0.0

File View Mode Help

Evidence Tree

LAPTOP-CO8V8FPO-20200211-084558.raw
Unrecognized file system [unknown type]

File List

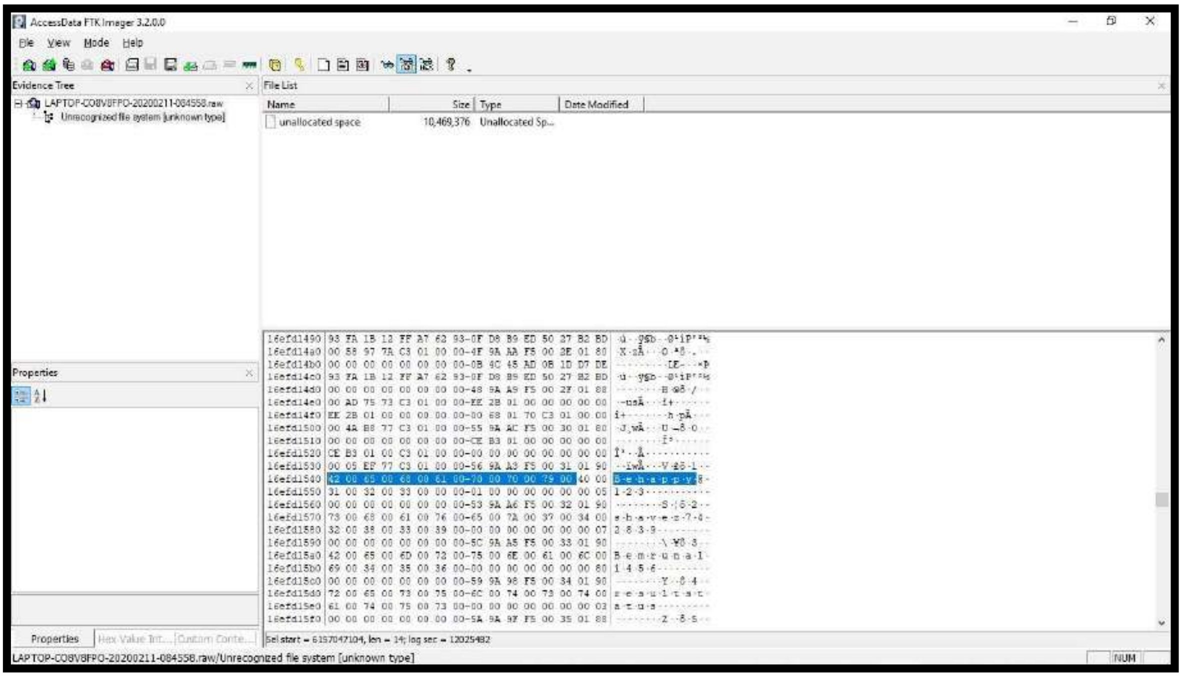
| Name | Size | Type | Date Modified |
|---|---|---|---|
| unallocated space | 10,469,376 | Unallocated Sp... | |

```
0666b44f0  00 00 00 00 08 00 00 00-18 00 00 00 00 00 00 00  ················
0666b4500  01 00 00 00 1F 93 0A 0B-00 00 00 00 E7 F7 BE F6  ············ç÷¾ö
0666b4510  10 00 00 00 00 00 00 00-08 00 00 00 00 00 00 00  ················
0666b4520  20 00 00 00 00 00 00 00-10 00 00 00 00 00 00 00  ················
0666b4530  10 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0666b4540  70 00 00 00 68 00 00 00-58 00 00 00 FF FF FF 7F  p···h···X···ÿÿÿ·
0666b4550  56 03 0F 00 02 D8 04 CD-8C D3 1B CD 57 AA 41 FE  V····Ø·Í·Ó·ÍWªAþ
0666b4560  7E 07 A8 C4 6C 51 A9 E0-6E 01 00 00 01 00 00 00  ~·¨ÄlQ©àn·······
0666b4570  35 00 00 00 22 5B 5C 22-68 5F 63 72 72 71 5C 22  5···"[\"h_crrq\"
0666b4580  2C 5B 6E 75 6C 6C 2C 34-31 2C 5C 22 6D 72 75 6E  ,[null,41,\"mrun
0666b4590  61 6C 69 62 61 67 64 65-32 37 40 67 6D 61 69 6C  alibagde27@gmail
0666b45a0  2E 63 6F 6D 5C 22 5D 5D-22 00 00 00 00 00 00 00  .com\"]]"·······
0666b45b0  48 04 00 00 10 00 01 00-00 00 00 00 00 00 00 00  H···············
0666b45c0  05 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0666b45d0  08 C4 08 33 A9 47 F8 4D-08 F6 22 A7 C3 28 0B D0  ·Ä·3©GøM·ö"§Ã(·Ð
0666b45e0  B7 4D 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ·M··············
0666b45f0  00 00 00 00 08 00 00 00-18 00 00 00 00 00 00 00  ················
0666b4600  01 00 00 00 1F 93 0A 0B-00 00 00 00 E6 F7 BE F6  ············æ÷¾ö
0666b4610  10 00 00 00 00 00 00 00-08 00 00 00 00 00 00 00  ················
0666b4620  20 00 00 00 00 00 00 00-10 00 00 00 00 00 00 00  ················
0666b4630  10 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0666b4640  B4 03 00 00 AC 03 00 00-9C 03 00 00 FF FF FF 7F  ´···¬·······ÿÿÿ·
0666b4650  35 03 0F 00 02 D9 04 CD-01 00 00 00 0A 00 00 00  5····Ù·Í········
```

Sel start = 1718306187, len = 25; log sec = 3356066

LAPTOP-CO8V8FPO-20200211-084558.raw/Unrecognized file system [unknown type]

**Fig 2. 1 Captured Email Id**



AccessData FTK Imager 3.2.0.0

Evidence Tree: LAPTOP-CO8V8FPO-20200211-084558.raw — Unrecognized file system [unknown type]

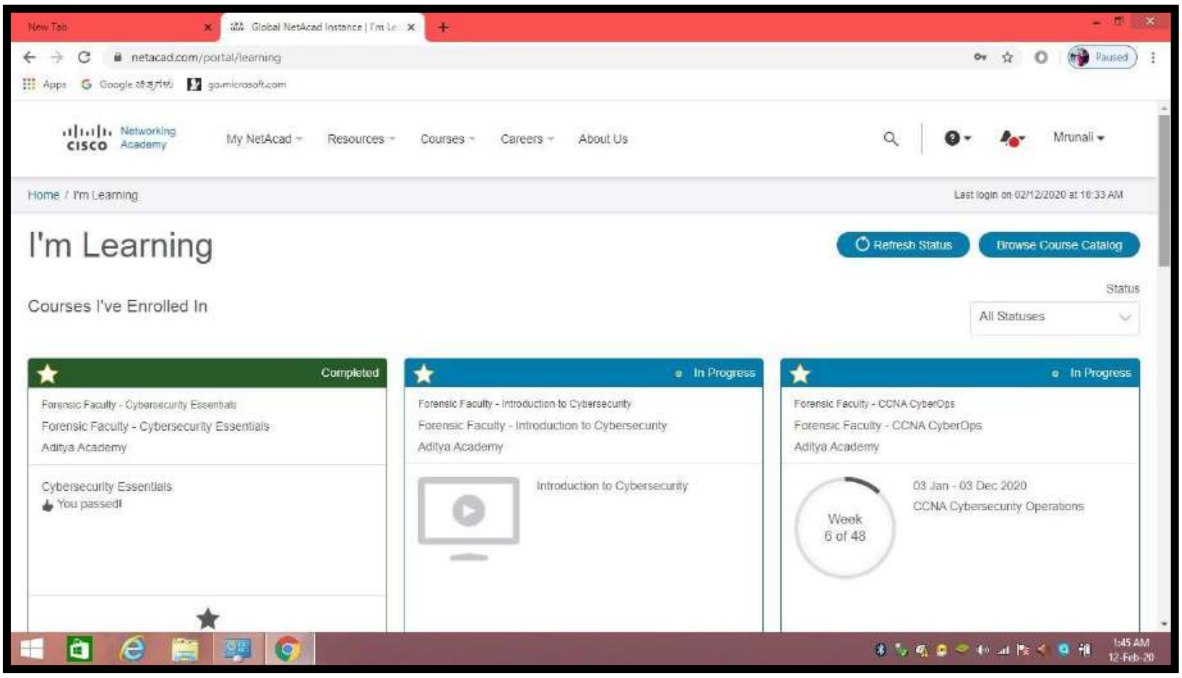
| Name | Size | Type | Date Modified |
|---|---|---|---|
| unallocated space | 10,469,376 | Unallocated Sp... | |

```
16efd1490 93 FA 1B 12 FF A7 62 93-0F D8 B9 ED 50 27 B2 BD  ·ú··ÿ§b··Ø¹íP'²½
16efd14a0 00 58 97 7A C3 01 00 00-4F 9A AA F5 00 2E 01 80  ·X·zÃ···O·ªõ·.··
16efd14b0 00 00 00 00 00 00 00 00-0B 4C 45 AD 0B 1D D7 DE  ·········LE-··×Þ
16efd14c0 93 FA 1B 12 FF A7 62 93-0F D8 B9 ED 50 27 B2 BD  ·ú··ÿ§b··Ø¹íP'²½
16efd14d0 00 00 00 00 00 00 00 00-48 9A A9 F5 00 2F 01 88  ········H·©õ·/··
16efd14e0 00 AD 75 73 C3 01 00 00-EE 2B 01 00 00 00 00 00  ·-usÃ···î+······
16efd14f0 EE 2B 01 00 00 00 00 00-00 68 01 70 C3 01 00 00  î+·······h·pÃ···
16efd1500 00 4A B8 77 C3 01 00 00-55 9A AC F5 00 30 01 80  ·J¸wÃ···U·¬õ·0··
16efd1510 00 00 00 00 00 00 00 00-CE B3 01 00 00 00 00 00  ········Î³······
16efd1520 CE B3 01 00 C3 01 00 00-00 00 00 00 00 00 00 00  Î³··Ã···········
16efd1530 00 05 EF 77 C3 01 00 00-56 9A A3 F5 00 31 01 90  ··ïwÃ···V·£õ·1··
16efd1540 42 00 65 00 68 00 61 00-70 00 70 00 79 00 40 00  B·e·h·a·p·p·y·@·
16efd1550 31 00 32 00 33 00 00 00-01 00 00 00 00 00 00 05  1·2·3···········
16efd1560 00 00 00 00 00 00 00 00-53 9A A6 F5 00 32 01 90  ········S·¦õ·2··
16efd1570 73 00 68 00 61 00 76 00-65 00 7A 00 37 00 34 00  s·h·a·v·e·z·7·4·
16efd1580 32 00 38 00 33 00 39 00-00 00 00 00 00 00 00 07  2·8·3·9·········
16efd1590 00 00 00 00 00 00 00 00-5C 9A A5 F5 00 33 01 90  ········\·¥õ·3··
16efd15a0 42 00 65 00 6D 00 72 00-75 00 6E 00 61 00 6C 00  B·e·m·r·u·n·a·l·
16efd15b0 69 00 34 00 35 00 36 00-00 00 00 00 00 00 00 80  i·4·5·6·········
16efd15c0 00 00 00 00 00 00 00 00-59 9A 98 F5 00 34 01 90  ········Y··õ·4··
16efd15d0 72 00 65 00 73 00 75 00-6C 00 74 00 73 00 74 00  r·e·s·u·l·t·s·t·
16efd15e0 61 00 74 00 75 00 73 00-00 00 00 00 00 00 00 03  a·t·u·s·········
16efd15f0 00 00 00 00 00 00 00 00-5A 9A 9F F5 00 35 01 88  ········Z··õ·5··
```

Sel start = 6157047104, len = 14; log sec = 12025482

LAPTOP-CO8V8FPO-20200211-084558.raw/Unrecognized file system [unknown type]

**Fig 2. 2 Captured Password**



netacad.com/portal/learning

Home / I'm Learning

Last login on 02/12/2020 at 10:33 AM

I'm Learning

Courses I've Enrolled In

Status: All Statuses

Completed — Forensic Faculty - Cybersecurity Essentials; Forensic Faculty - Cybersecurity Essentials; Aditya Academy; Cybersecurity Essentials; You passed!

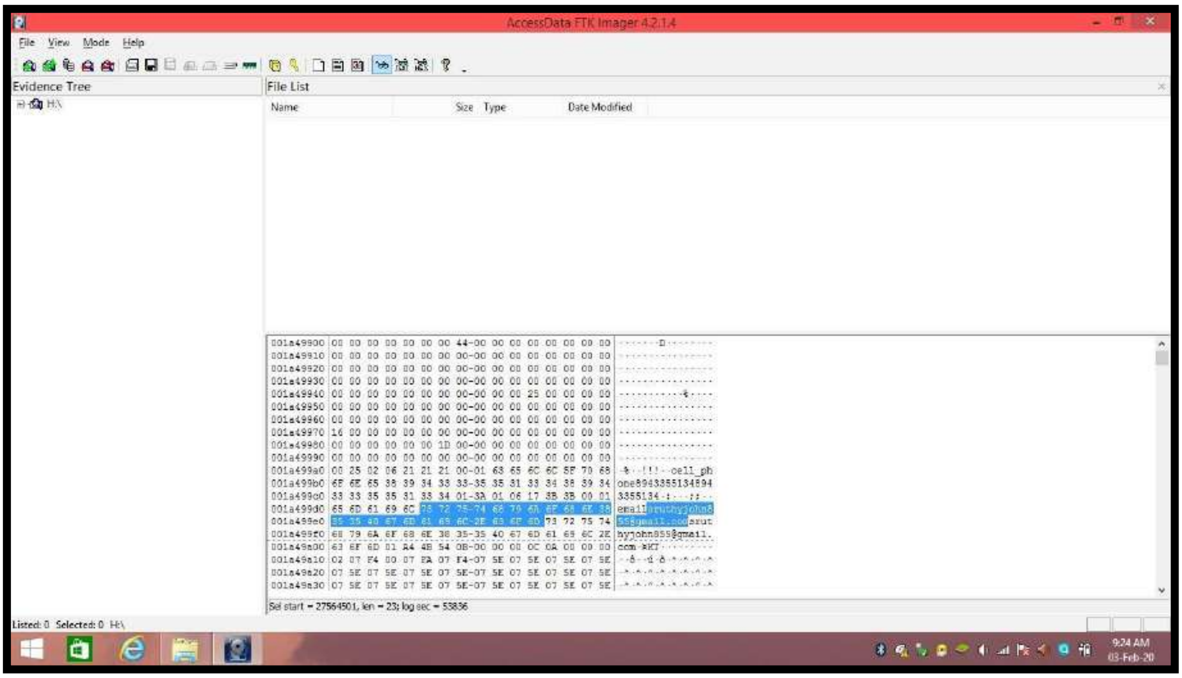
In Progress — Forensic Faculty - Introduction to Cybersecurity; Forensic Faculty - Introduction to Cybersecurity; Aditya Academy; Introduction to Cybersecurity

In Progress — Forensic Faculty - CCNA CyberOps; Forensic Faculty - CCNA CyberOps; Aditya Academy; Week 6 of 48; 03 Jan - 03 Dec 2020; CCNA Cybersecurity Operations

**Fig 2.3 Logged in Page**

## Sample 3

### Observation: Captured shine learning account id and password



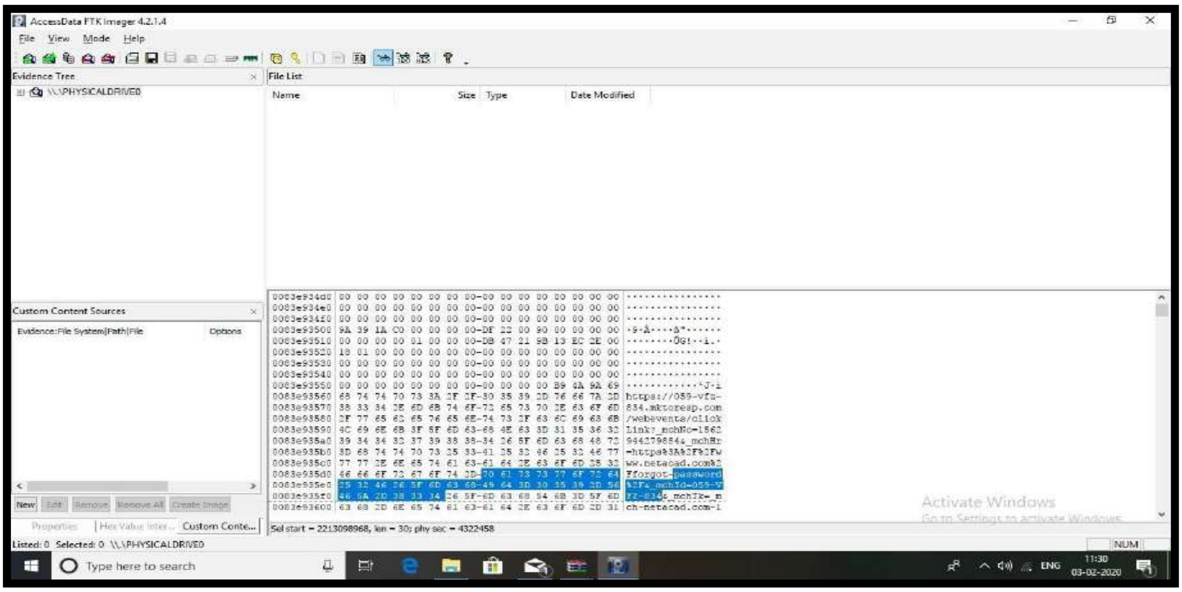
```
001a49900 00 00 00 00 00 00 00 44-00 00 00 00 00 00 00 00  ·······D········
001a49910 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49920 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49930 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49940 00 00 00 00 00 00 00 00-00 00 25 00 00 00 00 00  ··········%·····
001a49950 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49960 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49970 16 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a49980 00 00 00 00 00 00 1D 00-00 00 00 00 00 00 00 00  ················
001a49990 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
001a499a0 00 25 02 06 21 21 21 00-01 63 65 6C 6C 5F 70 68  ·%··!!!··cell_ph
001a499b0 6F 6E 65 38 39 34 33 33-35 35 31 33 34 38 39 34  one8943355134894
001a499c0 33 33 35 35 31 33 34 01-3A 01 06 17 3B 3B 00 01  3355134·:···;;··
001a499d0 65 6D 61 69 6C 73 72 75-74 68 79 6A 6F 68 6E 38  emailsruthyjohn8
001a499e0 35 35 40 67 6D 61 69 6C-2E 63 6F 6D 73 72 75 74  55@gmail.comsrut
001a499f0 68 79 6A 6F 68 6E 38 35-35 40 67 6D 61 69 6C 2E  hyjohn855@gmail.
001a49a00 63 6F 6D 01 A4 4B 54 0B-00 00 00 0C 0A 00 00 00  com·¤KT·········
001a49a10 02 07 F4 00 07 FA 07 F4-07 5E 07 5E 07 5E 07 5E  ··ô··ú·ô·^·^·^·^
001a49a20 07 5E 07 5E 07 5E 07 5E-07 5E 07 5E 07 5E 07 5E  ·^·^·^·^·^·^·^·^
001a49a30 07 5E 07 5E 07 5E 07 5E-07 5E 07 5E 07 5E 07 5E  ·^·^·^·^·^·^·^·^
```

Sel start = 27564501, len = 23; log sec = 53836

Listed: 0 Selected: 0 H:\

9:24 AM 03-Feb-20

Fig 3.1 captured email id


AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
Activate Windows
Go to Settings to activate Windows.
NUM
Type here to search
ENG
11:30
03-02-2020

```
0083e934d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e934e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e934f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e93500 9A 39 1A C0 00 00 00 00-DF 22 00 90 00 00 00 00  ·9·À····ß"······
0083e93510 00 00 00 00 01 00 00 00-DB 47 21 9B 13 EC 2E 00  ········ÛG!··ì.·
0083e93520 18 01 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e93530 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e93540 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0083e93550 00 00 00 00 00 00 00 00-00 00 00 00 B9 4A 9A 69  ············¹J·i
0083e93560 68 74 74 70 73 3A 2F 2F-30 35 39 2D 76 66 7A 2D  https://059-vfz-
0083e93570 38 33 34 2E 6D 6B 74 6F-72 65 73 70 2E 63 6F 6D  834.mktoresp.com
0083e93580 2F 77 65 62 65 76 65 6E-74 73 2F 63 6C 69 63 6B  /webevents/click
0083e93590 4C 69 6E 6B 3F 5F 6D 63-68 4E 63 3D 31 35 36 32  Link?_mchNc=1562
0083e935a0 39 34 34 32 37 39 38 38-34 26 5F 6D 63 68 48 72  944279884&_mchHr
0083e935b0 3D 68 74 74 70 73 25 33-41 25 32 46 25 32 46 77  =https%3A%2F%2Fw
0083e935c0 77 77 2E 6E 65 74 61 63-61 64 2E 63 6F 6D 25 32  ww.netacad.com%2
0083e935d0 46 66 6F 72 67 6F 74 2D-70 61 73 73 77 6F 72 64  Fforgot-password
0083e935e0 25 32 46 26 5F 6D 63 68-49 64 3D 30 35 39 2D 56  %2F&_mchId=059-V
0083e935f0 46 5A 2D 38 33 34 26 5F-6D 63 68 54 6B 3D 5F 6D  FZ-834&_mchTk=_m
0083e93600 63 68 2D 6E 65 74 61 63-61 64 2E 63 6F 6D 2D 31  ch-netacad.com-1
```

Sel start = 2213098968, len = 30; phy sec = 4322458

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 3.2 captured password

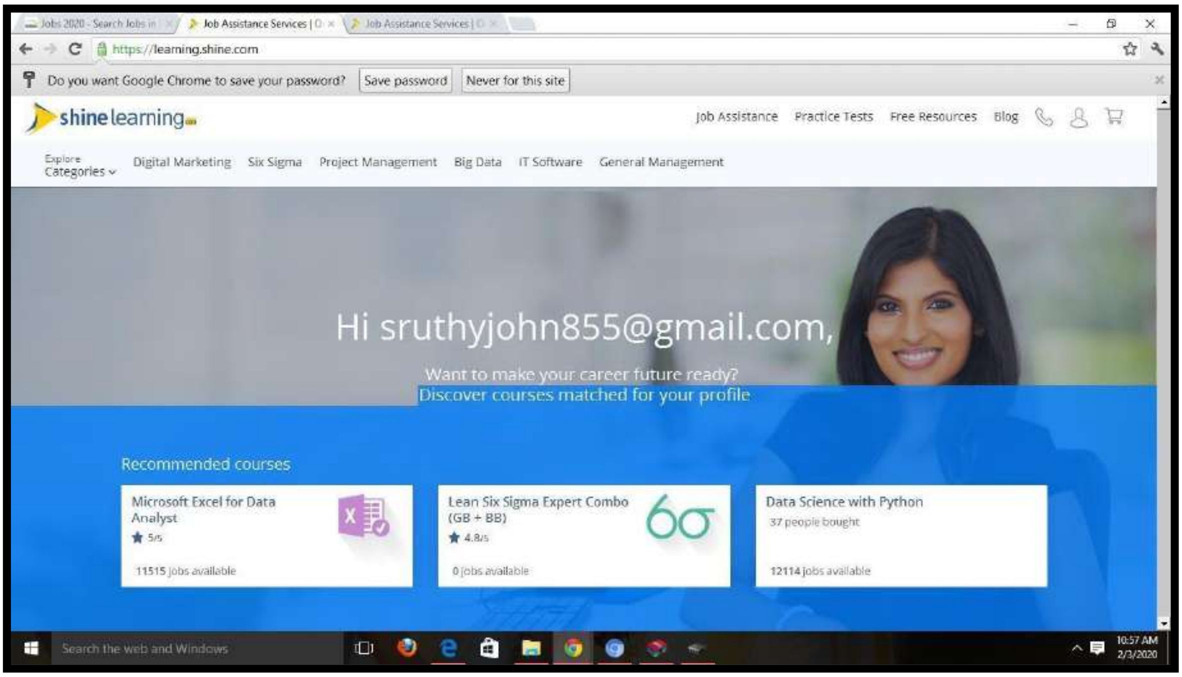
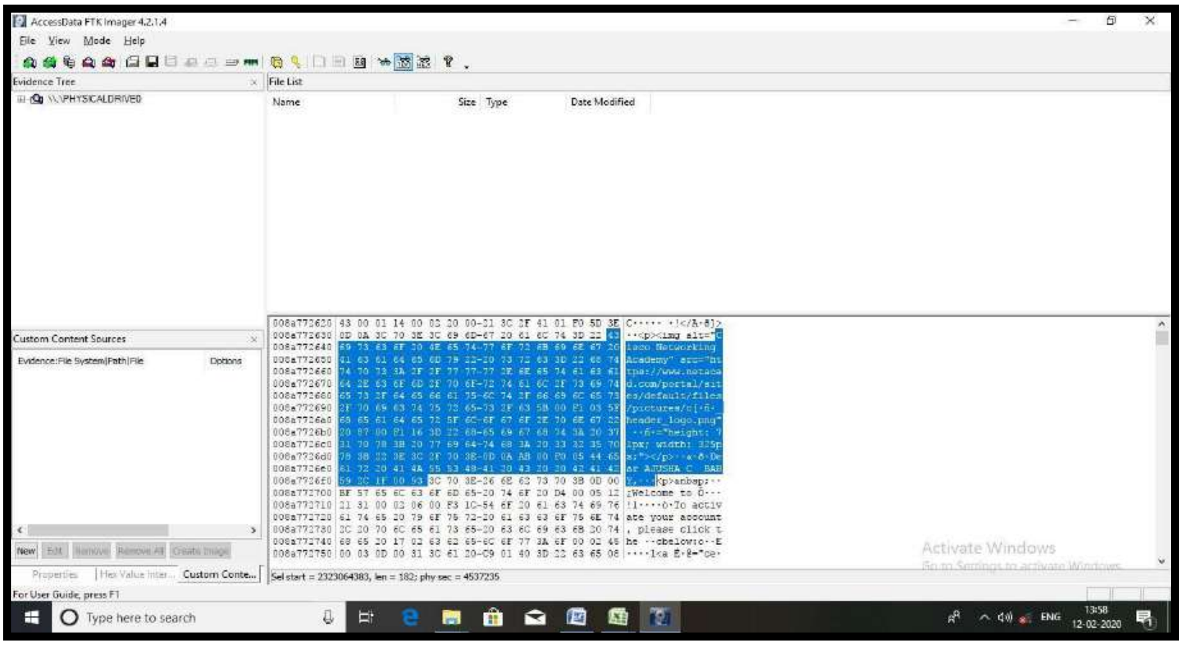

Jobs 2020 - Search Jobs in
Job Assistance Services | O
Job Assistance Services | O
https://learning.shine.com
Do you want Google Chrome to save your password?
Save password
Never for this site
shine learning
Job Assistance
Practice Tests
Free Resources
Blog
Explore Categories
Digital Marketing
Six Sigma
Project Management
Big Data
IT Software
General Management
Hi sruthyjohn855@gmail.com,
Want to make your career future ready?
Discover courses matched for your profile
Recommended courses
Microsoft Excel for Data Analyst
5/5
11515 jobs available
Lean Six Sigma Expert Combo (GB + BB)
4.8/5
0 jobs available
Data Science with Python
37 people bought
12114 jobs available
Search the web and Windows
10:57 AM
2/3/2020

Fig 3.3 Logged in Page

## Sample 4

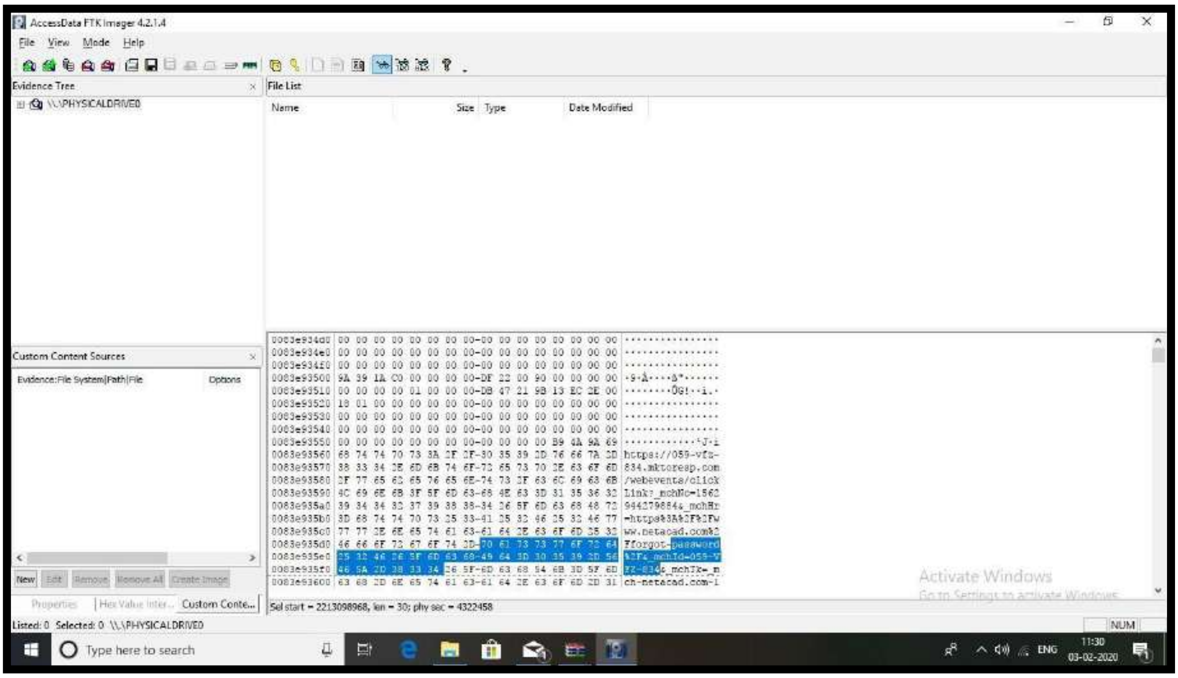
### Observation: Captured Password of Netacad Account



```
008a772620 43 00 01 14 00 02 20 00-21 3C 2F 41 01 F0 5D 3E  C······!</A·ð]>
008a772630 0D 0A 3C 70 3E 3C 69 6D-67 20 61 6C 74 3D 22 43  ··<p><img alt="C
008a772640 69 73 63 6F 20 4E 65 74-77 6F 72 6B 69 6E 67 20  isco Networking 
008a772650 41 63 61 64 65 6D 79 22-20 73 72 63 3D 22 68 74  Academy" src="ht
008a772660 74 70 73 3A 2F 2F 77 77-77 2E 6E 65 74 61 63 61  tps://www.netaca
008a772670 64 2E 63 6F 6D 2F 70 6F-72 74 61 6C 2F 73 69 74  d.com/portal/sit
008a772680 65 73 2F 64 65 66 61 75-6C 74 2F 66 69 6C 65 73  es/default/files
008a772690 2F 70 69 63 74 75 72 65-73 2F 63 5B 00 E1 03 5F  /pictures/c[·á·_
008a7726a0 68 65 61 64 65 72 5F 6C-6F 67 6F 2E 70 6E 67 22  header_logo.png"
008a7726b0 20 87 00 E1 16 3D 22 68-65 69 67 68 74 3A 20 37   ··á·="height: 7
008a7726c0 31 70 78 3B 20 77 69 64-74 68 3A 20 33 32 35 70  1px; width: 325p
008a7726d0 78 3B 22 3E 3C 2F 70 3E-0D 0A AB 00 F0 05 44 65  x;"></p>··«·ð·De
008a7726e0 61 72 20 41 4A 55 53 48-41 20 43 20 20 42 41 42  ar AJUSHA C  BAB
008a7726f0 59 2C 1F 00 93 3C 70 3E-26 6E 62 73 70 3B 0D 00  Y,···<p>&nbsp;··
008a772700 BF 57 65 6C 63 6F 6D 65-20 74 6F 20 D4 00 05 12  ¿Welcome to Ô···
008a772710 21 31 00 02 06 00 F3 1C-54 6F 20 61 63 74 69 76  !1····ó·To activ
008a772720 61 74 65 20 79 6F 75 72-20 61 63 63 6F 75 6E 74  ate your account
008a772730 2C 20 70 6C 65 61 73 65-20 63 6C 69 63 6B 20 74  , please click t
008a772740 68 65 20 17 02 63 62 65-6C 6F 77 3A 6F 00 02 45  he ··cbelow:o··E
008a772750 00 03 0D 00 31 3C 61 20-C9 01 40 3D 22 63 65 08  ····1<a É·@="ce·
```

Sel start = 2323064383, len = 182; phy sec = 4537235

Fig 4.1 Captured Email Id



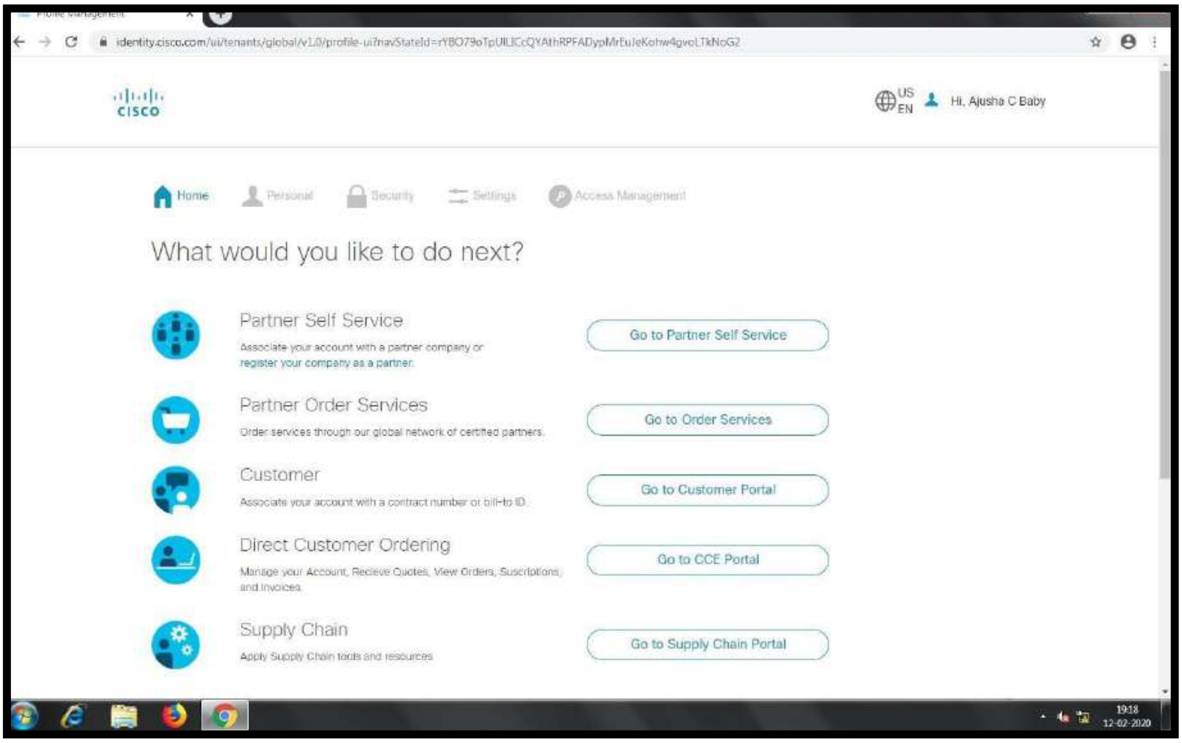
AccessData FTK Imager 4.2.1.4

Evidence Tree: \\.\PHYSICALDRIVE0

```
0083e934d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e934e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e934f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e93500 9A 39 1A C0 00 00 00 00-DF 22 00 90 00 00 00 00 ·9·À····ß"······
0083e93510 00 00 00 00 01 00 00 00-DB 47 21 9B 13 EC 2E 00 ········ÛG!··i.·
0083e93520 18 01 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e93530 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e93540 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0083e93550 00 00 00 00 00 00 00 00-00 00 00 00 B9 4A 9A 69 ············¹J·i
0083e93560 68 74 74 70 73 3A 2F 2F-30 35 39 2D 76 66 7A 2D https://059-vfz-
0083e93570 38 33 34 2E 6D 6B 74 6F-72 65 73 70 2E 63 6F 6D 834.mktoresp.com
0083e93580 2F 77 65 62 65 76 65 6E-74 73 2F 63 6C 69 63 6B /webevents/click
0083e93590 4C 69 6E 6B 3F 5F 6D 63-68 4E 63 3D 31 35 36 32 Link?_mchNc=1562
0083e935a0 39 34 34 32 37 39 38 38-34 26 5F 6D 63 68 48 72 944279884&_mchHr
0083e935b0 3D 68 74 74 70 73 25 33-41 25 32 46 25 32 46 77 =https%3A%2F%2Fw
0083e935c0 77 77 2E 6E 65 74 61 63-61 64 2E 63 6F 6D 25 32 ww.netacad.com%2
0083e935d0 46 66 6F 72 67 6F 74 2D-70 61 73 73 77 6F 72 64 Fforgot-password
0083e935e0 25 32 46 26 5F 6D 63 68-49 64 3D 30 35 39 2D 56 %2F&_mchId=059-V
0083e935f0 46 5A 2D 38 33 34 26 5F-6D 63 68 54 6B 3D 5F 6D FZ-834&_mchTk=_m
0083e93600 63 68 2D 6E 65 74 61 63-61 64 2E 63 6F 6D 2D 31 ch-netacad.com-1
```

Sel start = 2213098968, len = 30; phy sec = 4322458

**Fig 4. 2 Captured Password**



identity.cisco.com/ui/tenants/global/v1.0/profile-ui?navStateId=rYBO79oTpUlLlCcQYAthRPFADypMrEuJeKohw4gvoLTkNoG2

Hi, Ajusha C Baby

What would you like to do next?

Partner Self Service — Associate your account with a partner company or register your company as a partner. — Go to Partner Self Service

Partner Order Services — Order services through our global network of certified partners. — Go to Order Services

Customer — Associate your account with a contract number or bill-to ID. — Go to Customer Portal

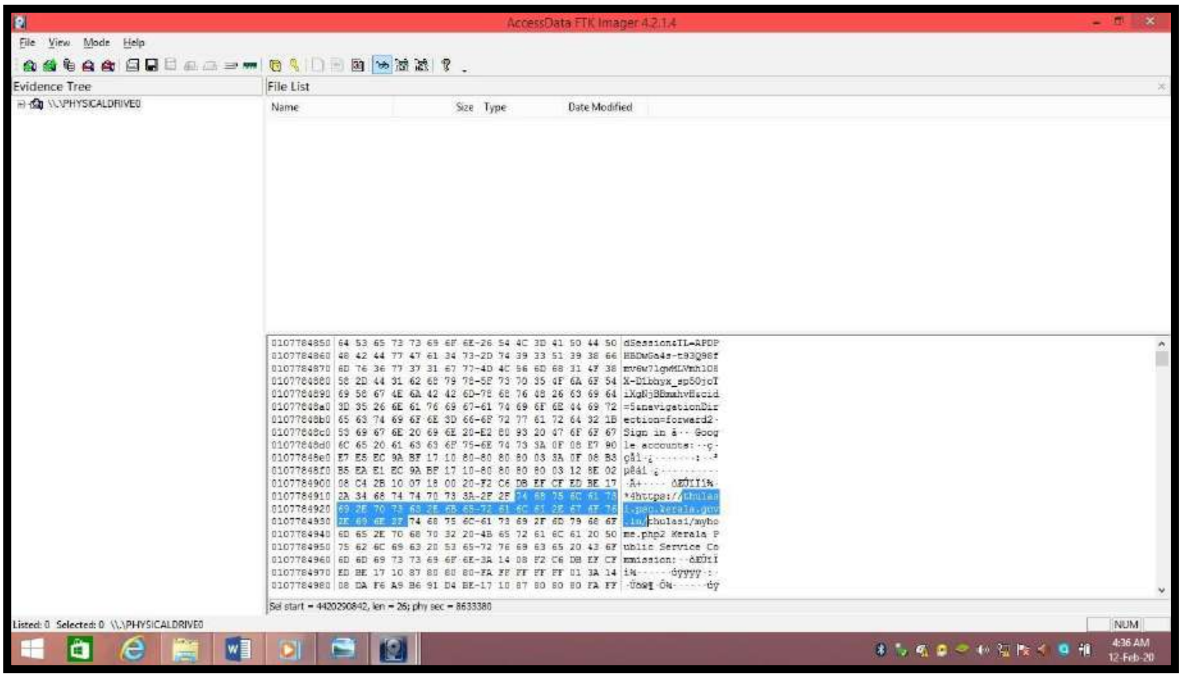
Direct Customer Ordering — Manage your Account, Recieve Quotes, View Orders, Suscriptions, and Invoices. — Go to CCE Portal

Supply Chain — Apply Supply Chain tools and resources — Go to Supply Chain Portal

**Fig 4.3 Logged in Page**

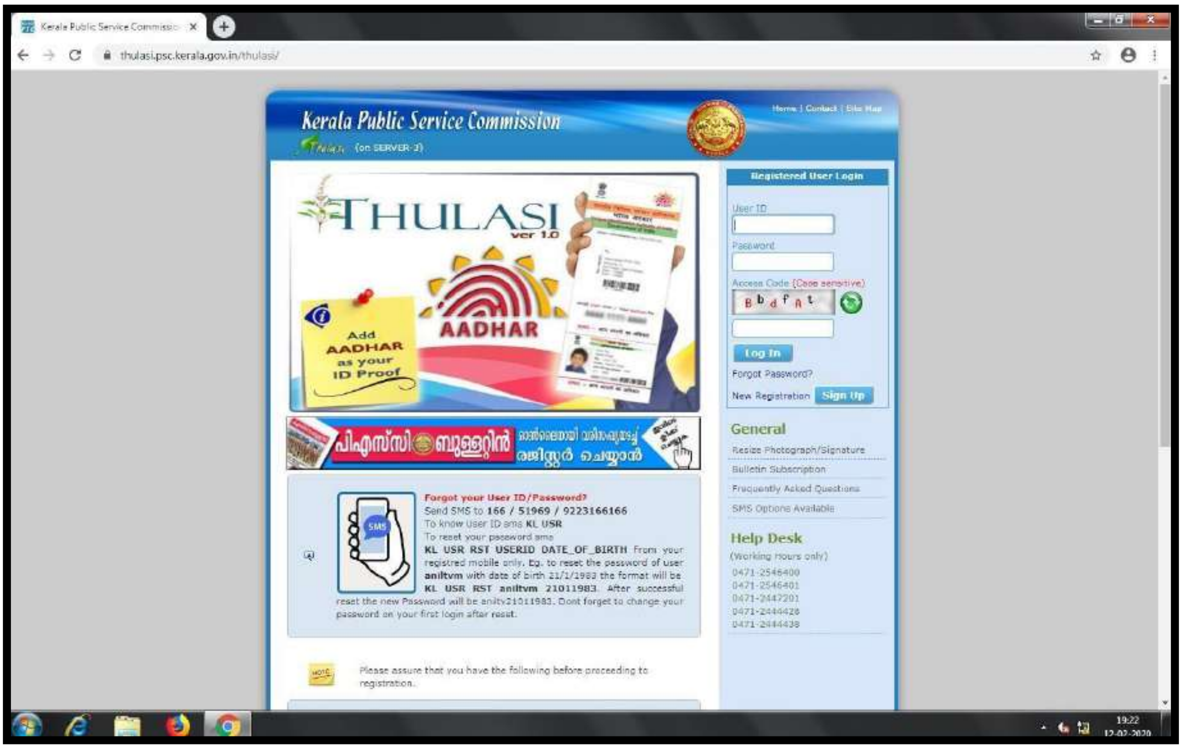
## Sample 5

### Observation: Captured Recently Used Website 1


AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0
NUM
4:36 AM
12-Feb-20

```
0107784850 64 53 65 73 73 69 6F 6E-26 54 4C 3D 41 50 44 50 dSession&TL=APDP
0107784860 48 42 44 77 47 61 34 73-2D 74 39 33 51 39 38 66 HBDwGa4s-t93Q98f
0107784870 6D 76 36 77 37 31 67 77-4D 4C 56 6D 68 31 4F 38 mv6w71gwMLVmh1O8
0107784880 58 2D 44 31 62 68 79 78-5F 73 70 35 4F 6A 6F 54 X-D1bhyx_sp5OjoT
0107784890 69 58 67 4E 6A 42 42 6D-78 68 76 48 26 63 69 64 iXgNjBBmxhvH&cid
01077848a0 3D 35 26 6E 61 76 69 67-61 74 69 6F 6E 44 69 72 =5&navigationDir
01077848b0 65 63 74 69 6F 6E 3D 66-6F 72 77 61 72 64 32 1B ection=forward2·
01077848c0 53 69 67 6E 20 69 6E 20-E2 80 93 20 47 6F 6F 67 Sign in â·· Goog
01077848d0 6C 65 20 61 63 63 6F 75-6E 74 73 3A 0F 08 E7 90 le accounts:··ç·
01077848e0 E7 E5 EC 9A BF 17 10 80-80 80 80 03 3A 0F 08 B3 çåì·¿·······:··³
01077848f0 B5 EA E1 EC 9A BF 17 10-80 80 80 80 03 12 8E 02 µêáì·¿··········
0107784900 08 C4 2B 10 07 18 00 20-F2 C6 DB EF CF ED BE 17 ·Ä+····òÆÛïÏí¾·
0107784910 2A 34 68 74 74 70 73 3A-2F 2F 74 68 75 6C 61 73 *4https://thulas
0107784920 69 2E 70 73 63 2E 6B 65-72 61 6C 61 2E 67 6F 76 i.psc.kerala.gov
0107784930 2E 69 6E 2F 74 68 75 6C-61 73 69 2F 6D 79 68 6F .in/thulasi/myho
0107784940 6D 65 2E 70 68 70 32 20-4B 65 72 61 6C 61 20 50 me.php2 Kerala P
0107784950 75 62 6C 69 63 20 53 65-72 76 69 63 65 20 43 6F ublic Service Co
0107784960 6D 6D 69 73 73 69 6F 6E-3A 14 08 F2 C6 DB EF CF mmission:··òÆÛïÏ
0107784970 ED BE 17 10 87 80 80 80-FA FF FF FF FF 01 3A 14 í¾······úÿÿÿÿ·:·
0107784980 08 DA F6 A9 B6 91 D4 BE-17 10 87 80 80 80 FA FF ·Úö©¶·Ô¾······úÿ
Sel start = 4420290842, len = 26; phy sec = 8633380
```

Fig 5.1 Captured Link of Website


Kerala Public Service Commissio
thulasi.psc.kerala.gov.in/thulasi/
Kerala Public Service Commission
Thulasi (on SERVER-3)
Home | Contact | Site Map
THULASI ver 1.0
Add AADHAR as your ID Proof
AADHAR
പിഎസ്‌സി ബുള്ളറ്റിൻ ഓൺലൈനായി വരിചേരുവാൻ രജിസ്റ്റർ ചെയ്യാൻ
Registered User Login
User ID
Password
Access Code (Case sensitive)
BbdfAt
Log In
Sign Up
19:22
12-02-2020

Forgot Password?

New Registration

General

Resize Photograph/Signature

Bulletin Subscription

Frequently Asked Questions

SMS Options Available

Help Desk

(Working Hours only)

0471-2546400
0471-2546401
0471-2447201
0471-2444428
0471-2444438

Forgot your User ID/Password?

Send SMS to **166 / 51969 / 9223166166**

To know User ID sms **KL USR**

To reset your password sms

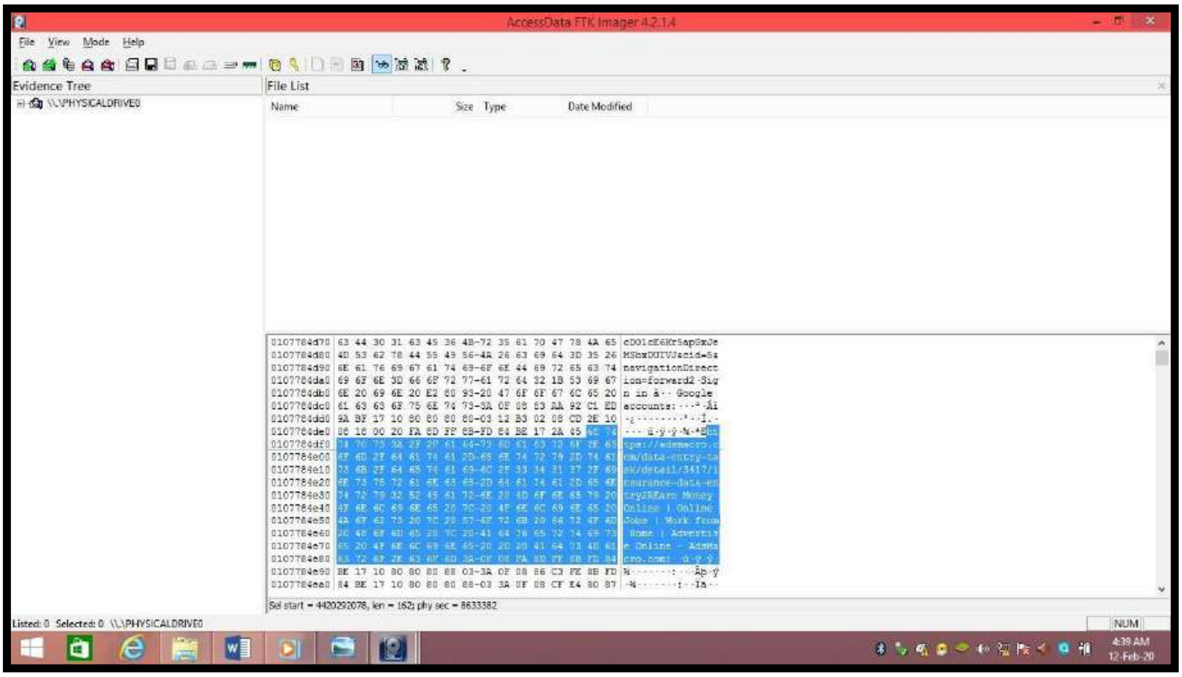
**KL USR RST USERID DATE_OF_BIRTH** From your registred mobile only. Eg. to reset the password of user **aniltvm** with date of birth 21/1/1983 the format will be **KL USR RST aniltvm 21011983**. After successful reset the new Password will be anitv21011983. Dont forget to change your password on your first login after reset.

Please assure that you have the following before proceeding to registration.

Fig 5.2 By Using the Link Entered Browsers

## Sample 6

**Observation: Captured Recently Used Website 2**

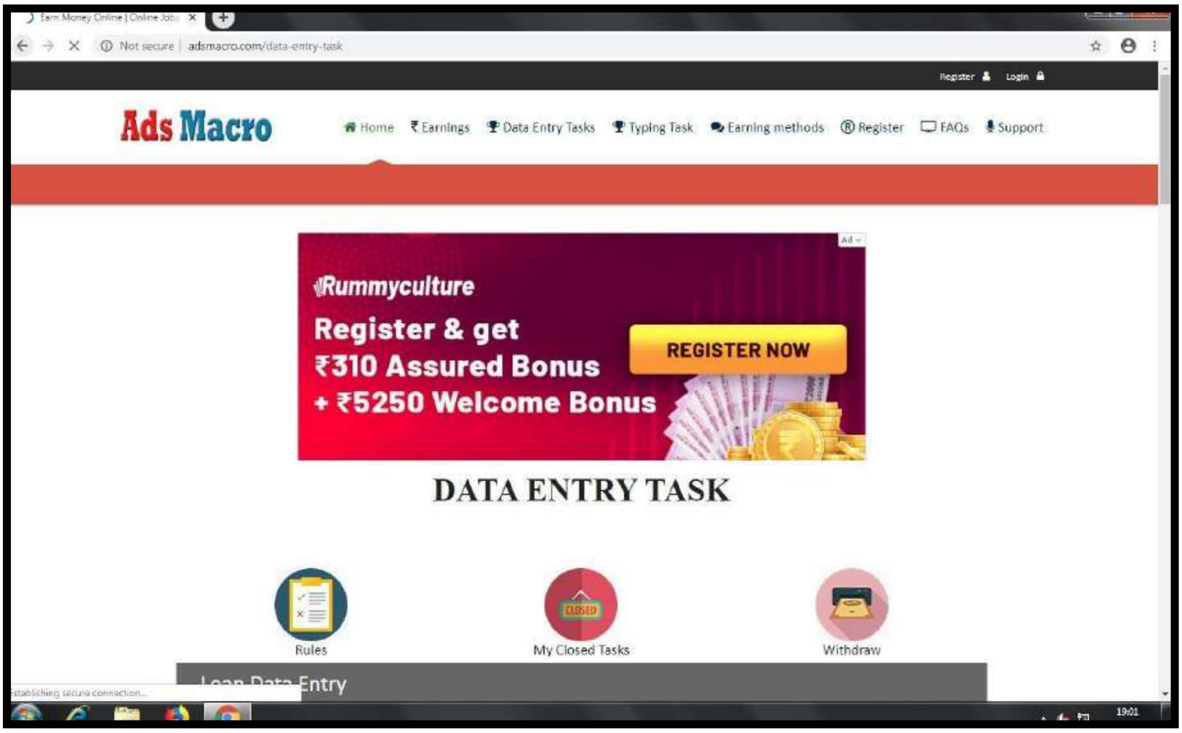


```
0107784d70  63 44 30 31 63 45 36 4B-72 35 61 70 47 78 4A 65  cD01cE6Kr5apGxJe
0107784d80  4D 53 62 78 44 55 49 56-4A 26 63 69 64 3D 35 26  MSbxDUIVJ&cid=5&
0107784d90  6E 61 76 69 67 61 74 69-6F 6E 44 69 72 65 63 74  navigationDirect
0107784da0  69 6F 6E 3D 66 6F 72 77-61 72 64 32 1B 53 69 67  ion=forward2·Sig
0107784db0  6E 20 69 6E 20 E2 80 93-20 47 6F 6F 67 6C 65 20  n in â·· Google 
0107784dc0  61 63 63 6F 75 6E 74 73-3A 0F 08 83 AA 92 C1 ED  accounts:···ª·Áí
0107784dd0  9A BF 17 10 80 80 80 80-03 12 B3 02 08 CD 2E 10  ·¿········³··Í.·
0107784de0  08 16 00 20 FA 8D FF 8B-FD 84 BE 17 2A 45 68 74  ··· ú·ÿ·ý·¾·*Eht
0107784df0  74 70 73 3A 2F 2F 61 64-73 6D 61 63 72 6F 2E 63  tps://adsmacro.c
0107784e00  6F 6D 2F 64 61 74 61 2D-65 6E 74 72 79 2D 74 61  om/data-entry-ta
0107784e10  73 6B 2F 64 65 74 61 69-6C 2F 33 34 31 37 2F 69  sk/detail/3417/i
0107784e20  6E 73 75 72 61 6E 63 65-2D 64 61 74 61 2D 65 6E  nsurance-data-en
0107784e30  74 72 79 32 52 45 61 72-6E 20 4D 6F 6E 65 79 20  try2REarn Money 
0107784e40  4F 6E 6C 69 6E 65 20 7C-20 4F 6E 6C 69 6E 65 20  Online | Online 
0107784e50  4A 6F 62 73 20 7C 20 57-6F 72 6B 20 66 72 6F 6D  Jobs | Work from
0107784e60  20 48 6F 6D 65 20 7C 20-41 64 76 65 72 74 69 73   Home | Advertis
0107784e70  65 20 4F 6E 6C 69 6E 65-20 2D 20 41 64 73 4D 61  e Online - AdsMa
0107784e80  63 72 6F 2E 63 6F 6D 3A-0F 08 FA 8D FF 8B FD 84  cro.com:··ú·ÿ·ý·
0107784e90  BE 17 10 80 80 80 88 03-3A 0F 08 86 C3 FE 8B FD  ¾·······:···Ãþ·ý
0107784ea0  84 BE 17 10 80 80 80 88-03 3A 0F 08 CF E4 80 87  ·¾·······:··Ïä··
```

Sel start = 4420292078, len = 162; phy sec = 8633382

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 6. 1 Captured Link of Website



DATA ENTRY TASK

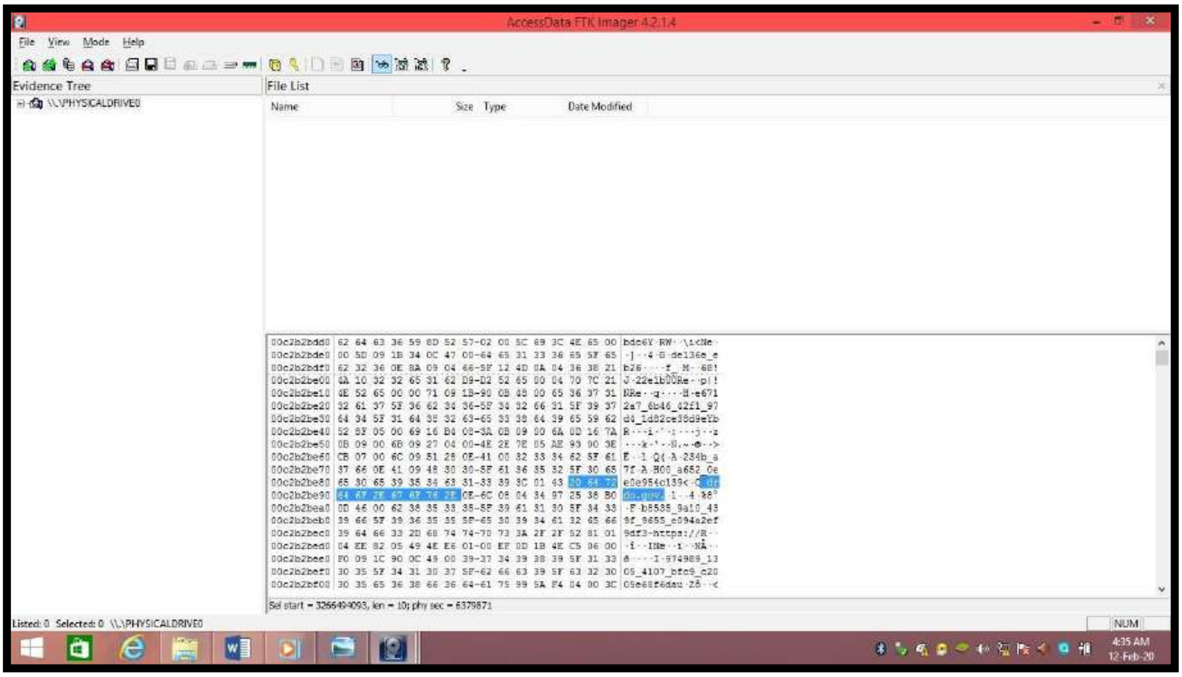
Loan Data Entry

Establishing secure connection...

Fig 6.2 Using the Link entered Browsers

## Sample 7

### Observation: Captured Recently Used Website 3



AccessData FTK Imager 4.2.1.4

Evidence Tree: \\.\PHYSICALDRIVE0

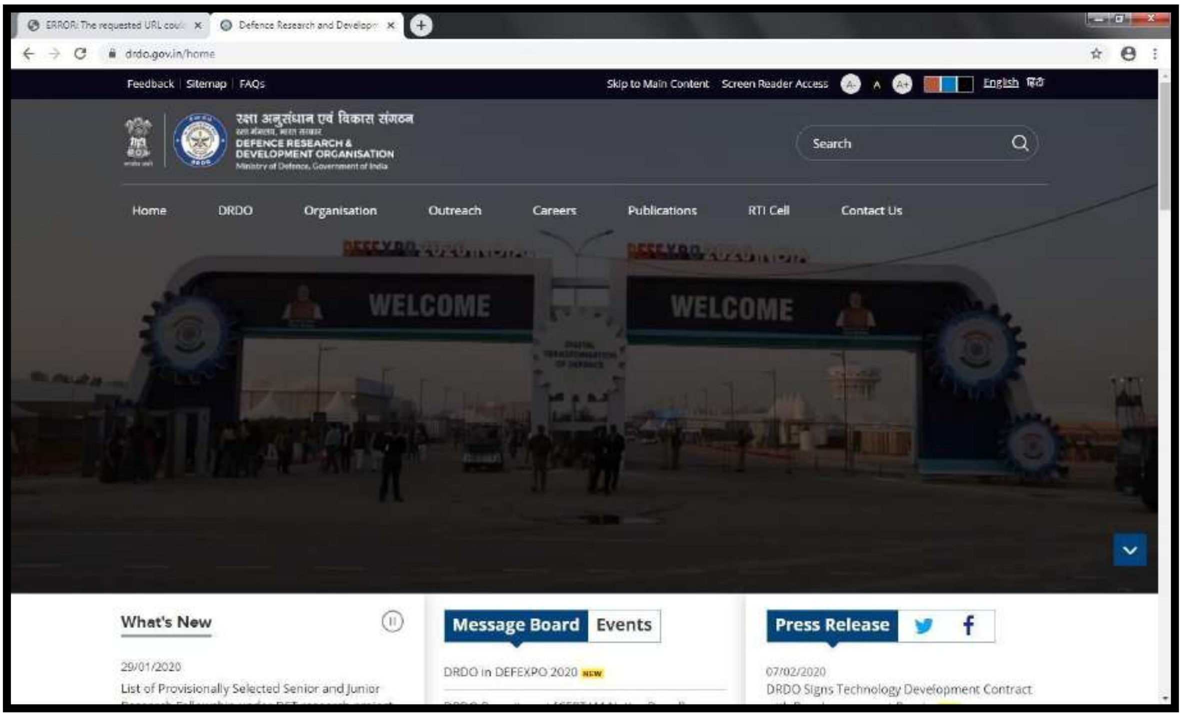
File List

```
00c2b2bdd0 62 64 63 36 59 8D 52 57-02 00 5C 69 3C 4E 65 00 bdc6Y·RW··\i<Ne·
00c2b2bde0 00 5D 09 1B 34 0C 47 00-64 65 31 33 36 65 5F 65 ·]··4·G·de136e_e
00c2b2bdf0 62 32 36 0E 8A 09 04 66-5F 12 4D 0A 04 36 38 21 b26····f_·M··68!
00c2b2be00 4A 10 32 32 65 31 62 D9-D2 52 65 00 04 70 7C 21 J·22e1bÙÒRe··p|!
00c2b2be10 4E 52 65 00 00 71 09 1B-90 0B 48 00 65 36 37 31 NRe··q····H·e671
00c2b2be20 32 61 37 5F 36 62 34 36-5F 34 32 66 31 5F 39 37 2a7_6b46_42f1_97
00c2b2be30 64 34 5F 31 64 38 32 63-65 33 38 64 39 65 59 62 d4_1d82ce38d9eYb
00c2b2be40 52 8F 05 00 69 16 B4 08-3A 0B 09 00 6A 0D 16 7A R···i·´·:···j··z
00c2b2be50 0B 09 00 6B 09 27 04 00-4E 2E 7E 05 AE 93 00 3E ···k·'··N.~·®··>
00c2b2be60 CB 07 00 6C 09 51 28 0E-41 00 32 33 34 62 5F 61 Ë··l·Q(·A·234b_a
00c2b2be70 37 66 0E 41 09 48 30 30-5F 61 36 35 32 5F 30 65 7f·A·H00_a652_0e
00c2b2be80 65 30 65 39 35 34 63 31-33 39 3C 01 43 20 64 72 e0e954c139<·C dr
00c2b2be90 64 6F 2E 67 6F 76 2E 0E-6C 08 04 34 97 25 38 B0 do.gov.·l··4·%8°
00c2b2bea0 0D 46 00 62 38 35 33 35-5F 39 61 31 30 5F 34 33 ·F·b8535_9a10_43
00c2b2beb0 39 66 5F 39 36 35 35 5F-65 30 39 34 61 32 65 66 9f_9655_e094a2ef
00c2b2bec0 39 64 66 33 2D 68 74 74-70 73 3A 2F 2F 52 81 01 9df3-https://R··
00c2b2bed0 04 EE 82 05 49 4E E6 01-00 EF 0D 1B 4E C5 06 00 ·î··INæ··ï··NÅ··
00c2b2bee0 F0 09 1C 90 0C 49 00 39-37 34 39 38 39 5F 31 33 ð····I·974989_13
00c2b2bef0 30 35 5F 34 31 30 37 5F-62 66 63 39 5F 63 32 30 05_4107_bfc9_c20
00c2b2bf00 30 35 65 36 38 66 36 64-61 75 99 5A F4 04 00 3C 05e68f6dau·Zô··<
```

Sel start = 3266494093, len = 10; phy sec = 6379871

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 7.1 Captured Link of Website



29/01/2020
List of Provisionally Selected Senior and Junior

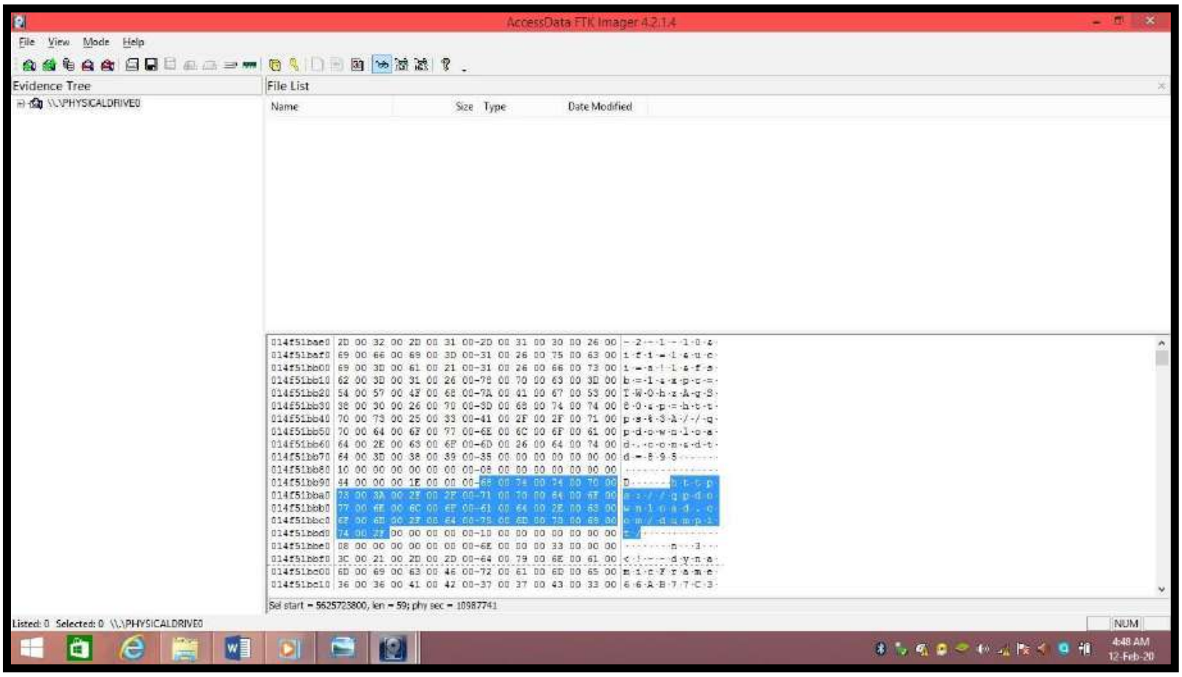
DRDO in DEFEXPO 2020

07/02/2020
DRDO Signs Technology Development Contract

Fig 7.2 Using the Link entered Browsers

## Sample 8

## Observation: Captured Recently used Website 4

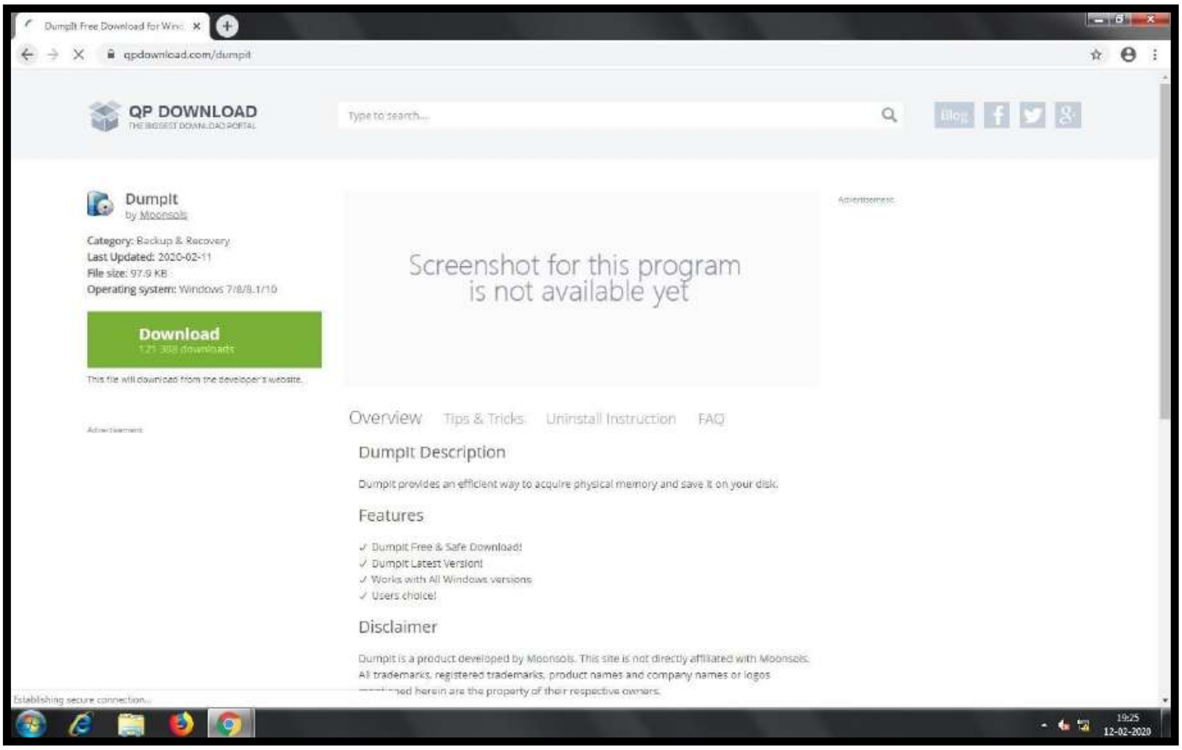


```
014f51bae0  2D 00 32 00 2D 00 31 00-2D 00 31 00 30 00 26 00  -·2·-·1·-·1·0·&·
014f51baf0  69 00 66 00 69 00 3D 00-31 00 26 00 75 00 63 00  i·f·i·=·1·&·u·c·
014f51bb00  69 00 3D 00 61 00 21 00-31 00 26 00 66 00 73 00  i·=·a·!·1·&·f·s·
014f51bb10  62 00 3D 00 31 00 26 00-78 00 70 00 63 00 3D 00  b·=·1·&·x·p·c·=·
014f51bb20  54 00 57 00 4F 00 68 00-7A 00 41 00 67 00 53 00  T·W·O·h·z·A·g·S·
014f51bb30  38 00 30 00 26 00 70 00-3D 00 68 00 74 00 74 00  8·0·&·p·=·h·t·t·
014f51bb40  70 00 73 00 25 00 33 00-41 00 2F 00 2F 00 71 00  p·s·%·3·A·/·/·q·
014f51bb50  70 00 64 00 6F 00 77 00-6E 00 6C 00 6F 00 61 00  p·d·o·w·n·l·o·a·
014f51bb60  64 00 2E 00 63 00 6F 00-6D 00 26 00 64 00 74 00  d·.·c·o·m·&·d·t·
014f51bb70  64 00 3D 00 38 00 39 00-35 00 00 00 00 00 00 00  d·=·8·9·5·······
014f51bb80  10 00 00 00 00 00 00 00-08 00 00 00 00 00 00 00  ················
014f51bb90  44 00 00 00 1E 00 00 00-68 00 74 00 74 00 70 00  D·······h·t·t·p·
014f51bba0  73 00 3A 00 2F 00 2F 00-71 00 70 00 64 00 6F 00  s·:·/·/·q·p·d·o·
014f51bbb0  77 00 6E 00 6C 00 6F 00-61 00 64 00 2E 00 63 00  w·n·l·o·a·d·.·c·
014f51bbc0  6F 00 6D 00 2F 00 64 00-75 00 6D 00 70 00 69 00  o·m·/·d·u·m·p·i·
014f51bbd0  74 00 2F 00 00 00 00 00-10 00 00 00 00 00 00 00  t·/·············
014f51bbe0  08 00 00 00 00 00 00 00-6E 00 00 00 33 00 00 00  ········n···3···
014f51bbf0  3C 00 21 00 2D 00 2D 00-64 00 79 00 6E 00 61 00  <·!·-·-·d·y·n·a·
014f51bc00  6D 00 69 00 63 00 46 00-72 00 61 00 6D 00 65 00  m·i·c·F·r·a·m·e·
014f51bc10  36 00 36 00 41 00 42 00-37 00 37 00 43 00 33 00  6·6·A·B·7·7·C·3·
```

Sel start = 5625723800, len = 59; phy sec = 10987741

Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0

Fig 8.1 captured link of website



DumpIt
by Moonsols

Category: Backup & Recovery
Last Updated: 2020-02-11
File size: 97.9 KB
Operating system: Windows 7/8/8.1/10

This file will download from the developer's website.

Screenshot for this program is not available yet

DumpIt Description

DumpIt provides an efficient way to acquire physical memory and save it on your disk.

Features

✓ DumpIt Free & Safe Download!
✓ DumpIt Latest Version!
✓ Works with All Windows versions
✓ Users choice!

Disclaimer

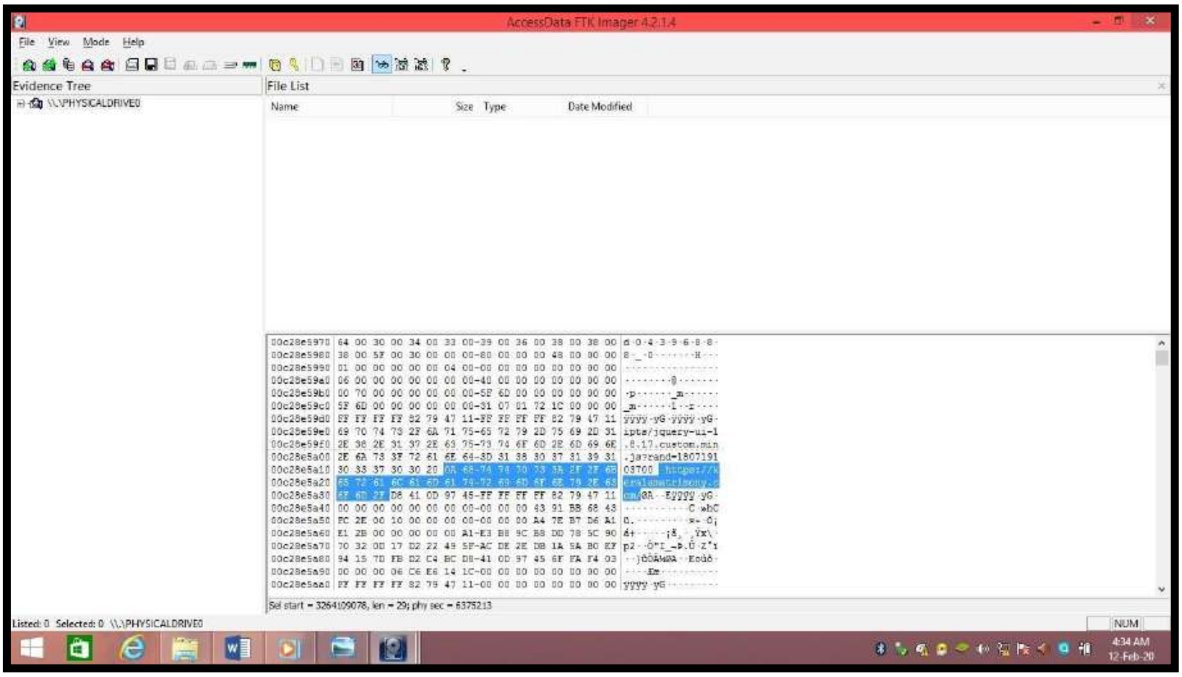
DumpIt is a product developed by Moonsols. This site is not directly affiliated with Moonsols. All trademarks, registered trademarks, product names and company names or logos mentioned herein are the property of their respective owners.

Establishing secure connection...

Fig 8.2 Captured Website Id

## Sample 9

### Observation: Captured Recently used Website 5

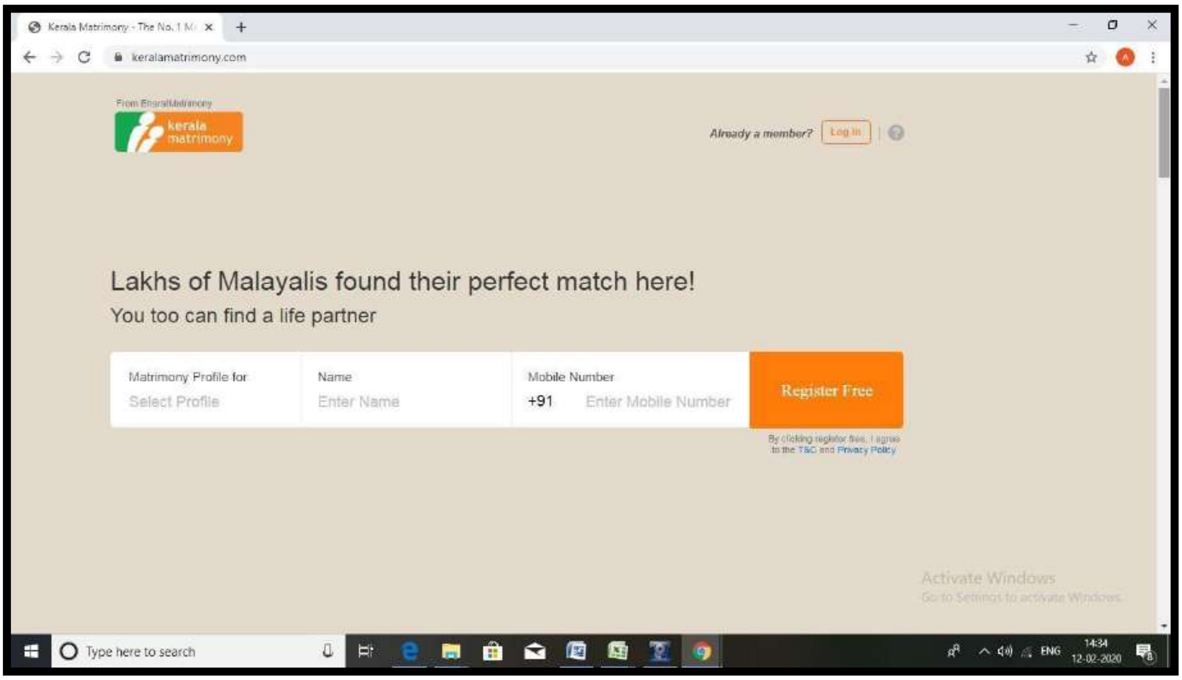


```
00c28e5970  64 00 30 00 34 00 33 00-39 00 36 00 38 00 38 00  d·0·4·3·9·6·8·8·
00c28e5980  38 00 5F 00 30 00 00 00-80 00 00 00 48 00 00 00  8·_·0·······H···
00c28e5990  01 00 00 00 00 00 04 00-00 00 00 00 00 00 00 00  ················
00c28e59a0  06 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00  ········@·······
00c28e59b0  00 70 00 00 00 00 00 00-5F 6D 00 00 00 00 00 00  ·p······_m······
00c28e59c0  5F 6D 00 00 00 00 00 00-31 07 01 72 1C 00 00 00  _m······1··r····
00c28e59d0  FF FF FF FF 82 79 47 11-FF FF FF FF 82 79 47 11  ÿÿÿÿ·yG·ÿÿÿÿ·yG·
00c28e59e0  69 70 74 73 2F 6A 71 75-65 72 79 2D 75 69 2D 31  ipts/jquery-ui-1
00c28e59f0  2E 38 2E 31 37 2E 63 75-73 74 6F 6D 2E 6D 69 6E  .8.17.custom.min
00c28e5a00  2E 6A 73 3F 72 61 6E 64-3D 31 38 30 37 31 39 31  .js?rand=1807191
00c28e5a10  30 33 37 30 30 20 0A 68-74 74 70 73 3A 2F 2F 6B  03700 ·https://k
00c28e5a20  65 72 61 6C 61 6D 61 74-72 69 6D 6F 6E 79 2E 63  eralamatrimony.c
00c28e5a30  6F 6D 2F D8 41 0D 97 45-FF FF FF FF 82 79 47 11  om/ØA··Eÿÿÿÿ·yG·
00c28e5a40  00 00 00 00 00 00 00 00-00 00 00 43 91 BB 68 43  ···········C·»hC
00c28e5a50  FC 2E 00 10 00 00 00 00-00 00 00 A4 7E B7 D6 A1  ü.·········¤~·Ö¡
00c28e5a60  E1 2B 00 00 00 00 00 A1-E3 B8 9C B8 DD 78 5C 90  á+·····¡ã¸·¸Ýx\·
00c28e5a70  70 32 00 17 D2 22 49 5F-AC DE 2E DB 1A 5A B0 EF  p2··Ò"I_¬Þ.Û·Z°ï
00c28e5a80  94 15 7D FB D2 C4 BC D8-41 0D 97 45 6F FA F4 03  ··}ûÒÄ¼ØA··Eoúô·
00c28e5a90  00 00 00 06 C6 E6 14 1C-00 00 00 00 00 00 00 00  ····Ææ··········
00c28e5aa0  FF FF FF FF 82 79 47 11-00 00 00 00 00 00 00 00  ÿÿÿÿ·yG·········
```

Sel start = 3264109078, len = 29; phy sec = 6375213

Listed: 0  Selected: 0  \\.\PHYSICALDRIVE0

Fig 9.1 Captured Link of Website



Lakhs of Malayalis found their perfect match here!

You too can find a life partner

Matrimony Profile for: Select Profile

Name: Enter Name

Mobile Number: +91 Enter Mobile Number

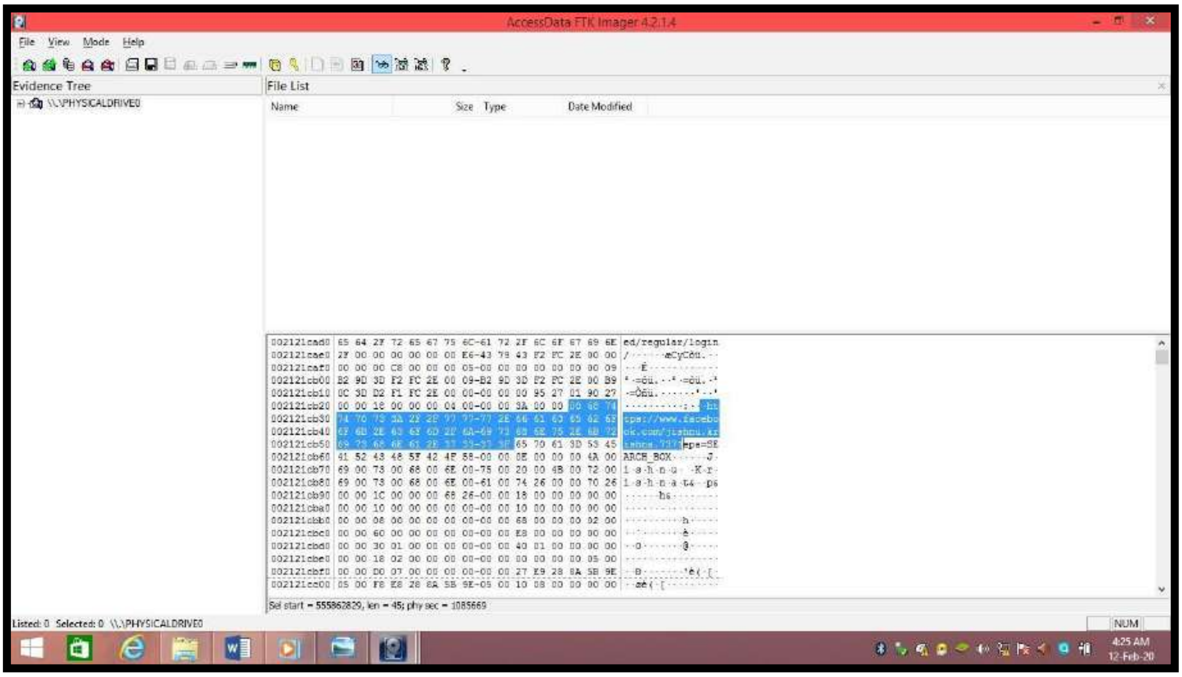
Register Free

By clicking register free, I agree to the T&C and Privacy Policy

Fig 9.2 Using the Link entered  Browsers

## Sample 10

## Captured recently used website 6


AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE0
File List
Name Size Type Date Modified
Listed: 0 Selected: 0 \\.\PHYSICALDRIVE0
NUM
4:25 AM
12-Feb-20

```
002121cad0  65 64 2F 72 65 67 75 6C-61 72 2F 6C 6F 67 69 6E  ed/regular/login
002121cae0  2F 00 00 00 00 00 00 E6-43 79 43 F2 FC 2E 00 00  /·······æCyCòü.··
002121caf0  00 00 00 C8 00 00 00 05-00 00 00 00 00 00 00 09  ···È············
002121cb00  B2 9D 3D F2 FC 2E 00 09-B2 9D 3D F2 FC 2E 00 B9  ²·=òü.··²·=òü.·¹
002121cb10  0C 3D D2 F1 FC 2E 00 00-00 00 00 95 27 01 90 27  ·=Òñü.·····'··'
002121cb20  00 00 18 00 00 00 04 00-00 00 3A 00 00 00 68 74  ··········:···ht
002121cb30  74 70 73 3A 2F 2F 77 77-77 2E 66 61 63 65 62 6F  tps://www.facebo
002121cb40  6F 6B 2E 63 6F 6D 2F 6A-69 73 68 6E 75 2E 6B 72  ok.com/jishnu.kr
002121cb50  69 73 68 6E 61 2E 37 33-37 3F 65 70 61 3D 53 45  ishna.737?epa=SE
002121cb60  41 52 43 48 5F 42 4F 58-00 00 0E 00 00 00 4A 00  ARCH_BOX······J·
002121cb70  69 00 73 00 68 00 6E 00-75 00 20 00 4B 00 72 00  i·s·h·n·u· ·K·r·
002121cb80  69 00 73 00 68 00 6E 00-61 00 74 26 00 00 70 26  i·s·h·n·a·t&··p&
002121cb90  00 00 1C 00 00 00 68 26-00 00 18 00 00 00 00 00  ······h&········
002121cba0  00 00 10 00 00 00 00 00-00 00 10 00 00 00 00 00  ················
002121cbb0  00 00 08 00 00 00 00 00-00 00 68 00 00 00 02 00  ··········h·····
002121cbc0  00 00 60 00 00 00 00 00-00 00 E8 00 00 00 00 00  ··`·······è·····
002121cbd0  00 00 30 01 00 00 00 00-00 00 40 01 00 00 00 00  ··0·······@·····
002121cbe0  00 00 18 02 00 00 00 00-00 00 00 00 00 00 05 00  ················
002121cbf0  00 00 D0 07 00 00 00 00-00 00 27 E9 28 8A 5B 9E  ··Ð·······'é(·[·
002121cc00  05 00 F8 E8 28 8A 5B 9E-05 00 10 08 00 00 00 00  ··øè(·[·········
Sel start = 555862829, len = 45; phy sec = 1085669
```

Fig 10.1 Captured Link of Website

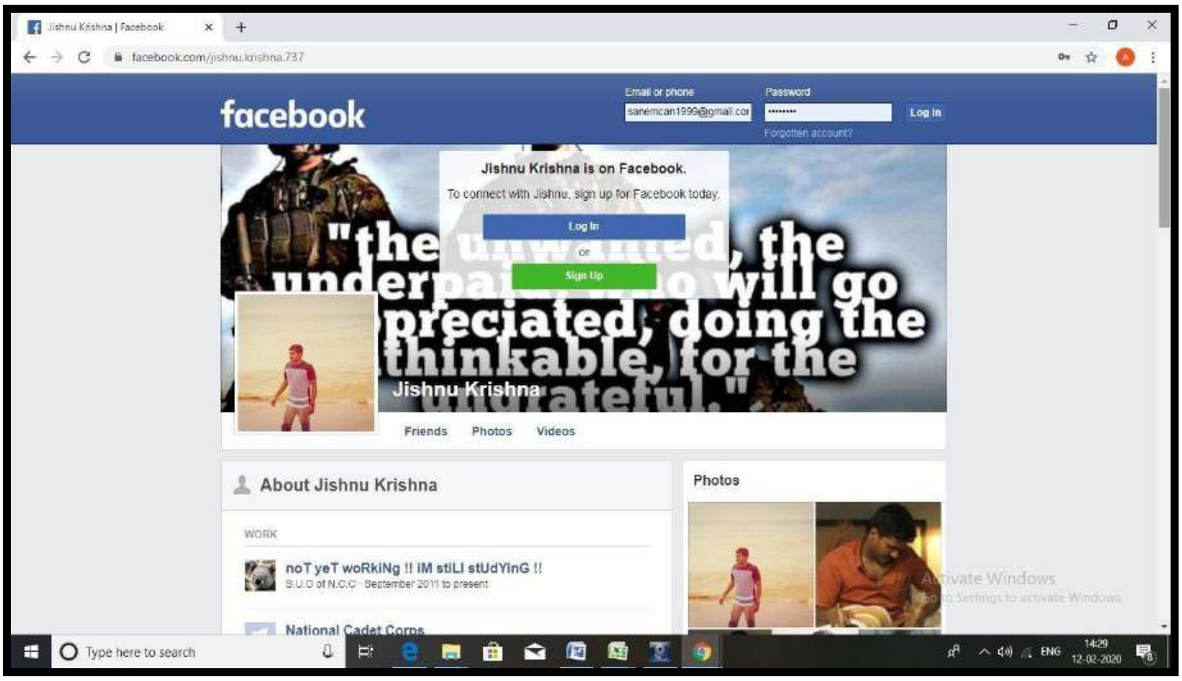

Jishnu Krishna | Facebook
facebook.com/jishnu.krishna.737
facebook
Email or phone
sanemcan1999@gmail.cor
Password
Log In
Forgotten account?
Jishnu Krishna is on Facebook.
To connect with Jishnu, sign up for Facebook today.
Log In
or
Sign Up
"the unwanted, the underpaid, who will go unappreciated, doing the unthinkable, for the ungrateful."
Jishnu Krishna
Friends
Photos
Videos
About Jishnu Krishna
WORK
noT yeT woRkiNg !! iM stiLl stUdYinG !!
S.U.O of N.C.C · September 2011 to present
National Cadet Corps
Photos
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
14:29
12-02-2020

Fig 10.2 Using the Link entered  Browsers

# CHAPTER VI

# RESULTS AND CONCLUSION

## RESULTS

| Samples | Result |
|---|---|
| Sample 1 | Captured Facebook id and password |
| Sample 2 | Captured password of Netacad account |
| Sample 3 | Captured shine learning account id and password |
| Sample 4 | Captured password of Netacad account |
| Sample 5 | Captured recently used website 1 |
| Sample 6 | Captured recently used website 2 |
| Sample 7 | Captured recently used website 3 |
| Sample 8 | Captured recently used website 4 |
| Sample 9 | Captured recently used website 5 |
| Sample 10 | Captured recently used website 6 |

Table 1.1 Results

## CONCLUSION:

By conducting the practical about the 10 samples the complete sample given positive results the password, email id and most recently visited website addresses .By the end of the study it gives a clear view how the FTK is user friendly to the user and help-full for the investigations. It also provides the guidance to the ametures to make the password cracking attacks easy. The recent surveys gives the sharp point that the free software's are dangerous to cyber forensic division in the way of increasing attacks tremendously. But an exact limit it is somewhat not readable format but also by using the different converting application we can claim it into human readable form.

# CHAPTER VII

## REFERENCES

1. Case Studies Cyber Security (www.Chub.Com)
2. Guidelines Of Accessdata FTK Imager 4.2.1
3. Digital Forensic by Dr. Nilakshi Jain and Dr. Dhananjayr. Kalbande
4. 23 Free Forensic Investigation Tools (Www.Geekflare.Com)
5. SANS Institute .Memory Forensics For Incident Response
6. Scheier, Bruce (2007-11-01). " Secure Passwords Keep You Safer"
7. Dixon, Phillip D (December 2005) "An Overview of Computer Forensics.Ieeepotenials" IEEE 24(5):8.
8. Casey, Eoghan (Fall 2002)."Practical Approaches to Recovering Encrypted Digital Evidence. International Journal of Digital Evidence. Utica, New York: Economic Crime Institute, Utica College.
9. Top 20 Free Digital Forensic Tools (Techtalk.Gfi.Com)
10. Passwords Crakong References
11. IEEE Digital Library
12. www.Techradar.Com
13. www.Dumit.Wikipedia.Com
14. www.Raw Images Capturing Tools.Com
15. www.Tools For Password Cracking.Com