Digital Intelligence

mastering the science of digital forensics

FRED SERVER

INDIRA GANDHI DELHI TECHNICAL UNIVERSITY FOR WOMEN

EDUCATION - EMPLOYMENT - EMPOWERMENT

आपो दीपो भव

ISEA

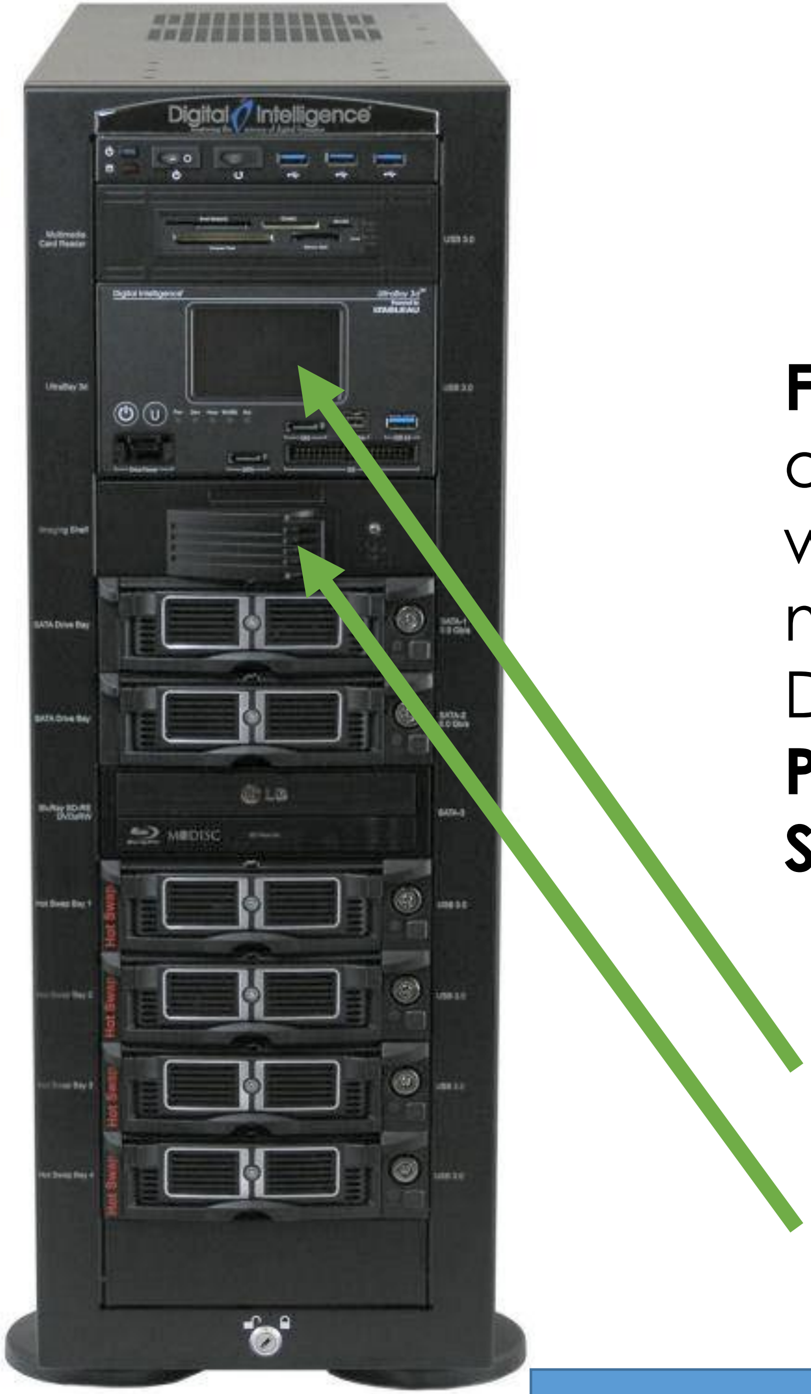
4th June, 2016

INDEX

1. Fred Introduction
    1. Ultrabay 3d Write Protected Imaging Bay
    2. Ventilated Imaging Shelf
2. The Complete Forensic Hardware Solution
3. Fast, Functional And Flexible
4. Network Functionality Built In
5. Baseline Fred Specifications
6. Toolbox Containing
7. Signals And Power Cables
8. Software
9. Proposed Experiments

FRED

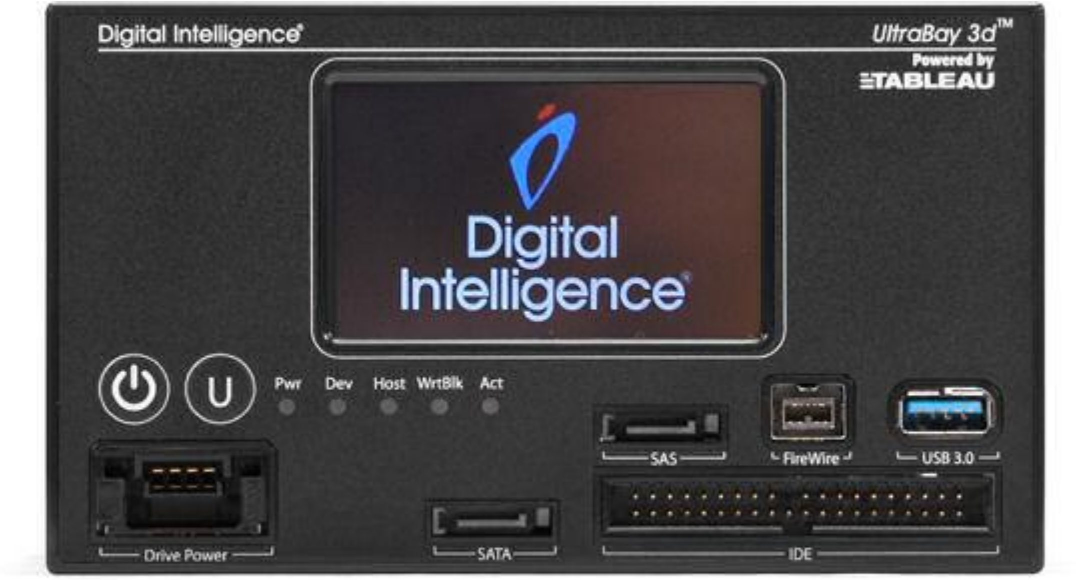
FRED is our **F**orensic **R**ecovery of **E**vidence **D**evice. The FRED family of forensic workstations are highly integrated, flexible and modular forensic platforms and now include Digital Intelligence's exclusive **UltraBay 3D Write Protected Imaging Bay** and **Ventilated Imaging Shelf**.



UltraBay 3D Write Protected Imaging Bay

Ventilated Imaging Shelf.

UltraBay 3D Write Protected Imaging Bay



- All front panel connectors are write blocked, which make for easy connections to drives being imaged. Simply connect the appropriate signal and drive power cables, start your imaging software, and acquire data. Drive power connections have been improved through the use of the new 3M style power connector.
- Firmware updates are easily applied using the Tableau Firmware Update (TFU) utility. TFU has been rewritten to enable firmware updates via the USB 3.0 host interface connection and features an exclusive firmware update "U" button, ensuring firmware updates are confidently managed.

UltraBay 3D Write Protected Imaging Bay

- The industry's first USB 3.0 integrated forensic bridge.
- Completely integrated / internal system solution.
- Integrated Write Blocked (Read-Only) Ports:
  - SAS
  - SATA
  - IDE
  - USB 3.0/2.0/1.1
  - FireWire 400/800
- Touch screen with a graphical user interface (GUI) for acquisition process monitoring.
- Full multi-LUN FireWire acquisition support is provided for Write Protected imaging of Apple Mac systems booted to FireWire device mode.
- Firmware updates available at no charge through Tableau Firmware Update.
- Full HPA/DCO support for SATA and IDE devices.
- FireWire write-blocked port has 9-pin FW800 connector and supports both FW400 and FW800 devices.

Ventilated Imaging Shelf

- Selected FRED systems include our ventilated imaging shelf for maximum drive cooling during the imaging process:
- Integrated Retractable imaging shelf (fully retracts into the system when not in use).
- Dual fans for maximum cooling and surface coverage.
- Auto On/Off switch when shelf is opened or closed.
- Slotted, cushioned, non-conductive, non-skid, surface supports all popular drive sizes (3-1/2", 2-1/2", 1.8", etc).

The Complete Forensic Hardware Solution

- FRED systems are optimized for stationary laboratory acquisition and analysis. Simply remove the hard drive(s) from the suspect system and plug them into FRED and acquire the digital evidence. FRED will acquire data directly from IDE/EIDE/ATA/SATA/ATAPI/SAS/Firewire/USB hard drives and storage devices and save forensic images to Blu-Ray, DVD, CD or hard drives. FRED systems also acquire data from Blu-Ray, CD-ROM, DVD-ROM, Compact Flash, Micro Drives, Smart Media, Memory Stick, Memory Stick Pro, xD Cards, Secure Digital Media and Multimedia Cards. Furthermore, with the optional tape drive FRED is capable of archiving to or acquiring evidence from LTO Ultrium 5 tapes. All FRED systems include the UltraBay, front panel connections, and removable drive trays so there is no need to open up the processing system to install drives or crawl around the back of the unit to attach devices.

Fast, Functional and Flexible

- Standard FRED systems come with three high speed drives (two SSDs and one 7200rpm mechanical). The first SSD is used for your Operating System(s), forensic acquisition and processing tools, the second SSD as a Temp/Cache/DataBase resource and the third as a work drive for restoring and processing digital evidence. FRED comes pre-installed with Windows 10 Professional on the Primary Drive. Additionally, a fully-loaded, pre-configured Suse Linux installation image is also included on factory restore Blu-ray for installation if desired. All three drives are supplied in shock-mounted removable drive trays. Most FRED Systems also come with integrated hot-swappable IDE and SATA bays to enable rapid installation and removal of evidence storage drives without the need for rebooting the system.

Network Functionality Built In

- All FRED systems can be connected directly to a network (10/100/1000 Mb ethernet) for use as a standard workstation or file server when not processing or acquiring data.

Baseline FRED Specifications

- 23 3/4" High, 8 3/8" Wide, 25 1/4" Deep - 80 lbs
- Intel Core i7-5820K CPU (Hex Core Processor), 3.3 GHz, 10MB Intel Smart Cache, 5 GT/s DMI
- 32 GB (4x8GB)PC3-17000 DDR4 2133 MHz Memory
- 1 x 256 GB Solid State SATA III Drive - OS Drive
- 1 x 128 GB Solid State SATA III Drive - Temp/Cache/DB Drive
- 1 x 2.0 TB 7200 RPM SATA III Hard Drive - Data Drive installed in HotSwap Bay1
- Nvidia GTX 750Ti 2GB 128 bit DDR5 PCI-Express Video Card with 1 VGA (D-Dub), 1 HDMI, and 2 DVI ports - supports up 4 displays
- 22" WideScreen LCD Monitor with Built-in Speakers

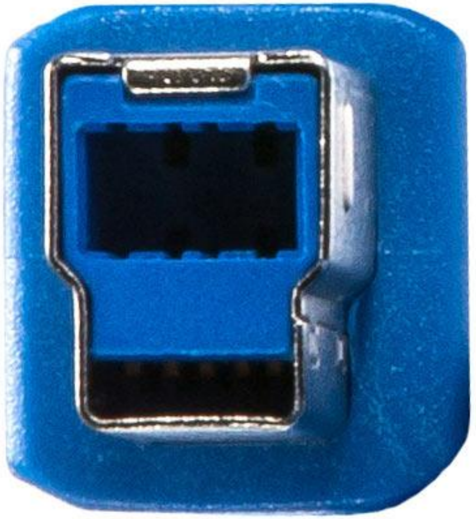
- **Windows 10 Professional (64 bit)**
  Also includes: SUSE Professional Linux (64 bit)
- **Hardware Write Blocking:**
  Digital Intelligence UltraBay 3d Hardware Write-Blocker with touch screen display:
- Integrated IDE Drive Write Blocker
- Integrated SATA Drive Write Blocker
- Integrated SAS Drive Write Blocker
- Integrated USB 3.0/2.0 Write Blocker
- Integrated FireWire IEEE 1394b Write Blocker
- Digital Intelligence Integrated Forensic Media Card Reader - Read-Only and Read/Write switchable

- **Detailed System Specifications:**
  ATX Tower Case 12 x 5 1/4" Bays
  1100 Watt Modular power supply
  i7 Motherboard with Intel X99 Chipset
  7 PCI-Express 3.0(x16) Slots
  8 ports Intel 6 Gb/s SATA Controller
  1 port Intel SATA Express Controller (or 2 x SATA 6 Gb/s ports)
  1 port ASMedia SATA Express Controller (or 2 x SATA 6 Gb/s ports)
  8 Channel High Definition Audio CODEC featuring Crystal Sound 2
  2 RJ45 LAN ports (Intel I210-AT, 1 x Gigabit LAN Intel I218LM, 1 x Gigabit LAN Controllers)
  2 eSATA 6 Gb/s ports - ASMedia controller
  14 USB 3.0/2.0 ports - 11 Back Mounted, 3 Front Mounted
  2 USB 3.1 ports - 2 Back Mounted
  1 Write Blocked USB 3.0/2.0 port - Front Mounted
  2 FireWire IEEE 1394b (800 MB/s) ports - 1 Back Mounted, 1 Front Mounted(Write Blocked)
  2 x Shock Mounted SATA Removable Hard Drive Bays (IDE Capable)
  4 x HotSwap Shock Mounted Universal (IDE/SATA compatible) Removable Hard Drive Bays
  BD-R/BD-RE/DVD+-RW/CD+-RW Blu-ray Burner Dual-Layer Combo Drive
  Extendable/Retractable Imaging Workshelf with integrated ventilation
- 103 key Keyboard and Mouse Combo - Wireless
- Toolbox containing: Adapters, Cables, Digital Camera, Security Screwdriver Set and OEM Documents
- Other Software included: Symantec Ghost and CD Authoring Software
- Warranty 1 year parts and labor

Toolbox Containing

- **CD Case:** Containing system restore media.
- **System Keys:** For removeable hard drive bays and front case bezel.
- **Adapters and Cables:** Cables and adapters to image and process internal/external drives including SAS, SATA, IDE, microSATA, SATA LIF, MacBook Air Blade Type SSDs, mini/micro SSD cards, 1.8 inch IDE (iPod) and 2.5 inch IDE (laptop).
- **Digital Camera:** Useful to document your suspects environment and hardware.
- **Security Screwdriver Set:** A varied assortment of popular security bits for opening computer enclosures that may have been locked down in a corporate environment.

SIGNALS AND POWER CABLES



TC-USB3

The TC-USB3 is a three foot long cable with a USB 3.0-A (9-pin) connector on one end and a USB 3.0-B (9-pin) connector on the other end.

Compatible With:

T8u, T35u, T35689iu TD2u, TD3

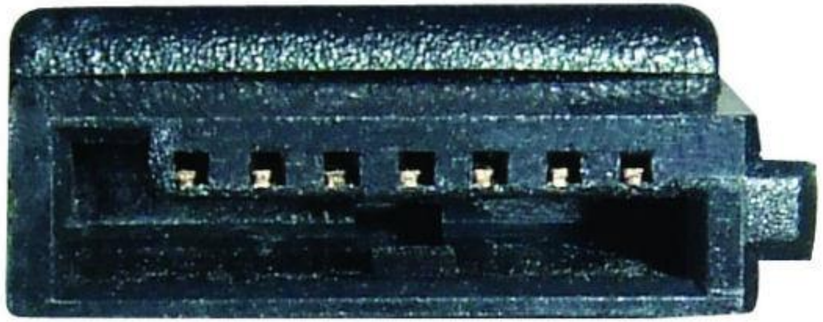
TC4-8-R2

The TC4-8-R2 is an eight inch long drive signal cable with a unified SATA/SAS signal and power to a SATA/SAS signal and 3M male power connector.

Compatible With:
T35u, T35689iu, TD2u, TD3, TDPX6

TC3-8

The TC3-8 is a standard, eight inch long SATA signal cable.



Compatible With:

T35u, T35es-R2, T35is, T35689iu, TD2u, TD3

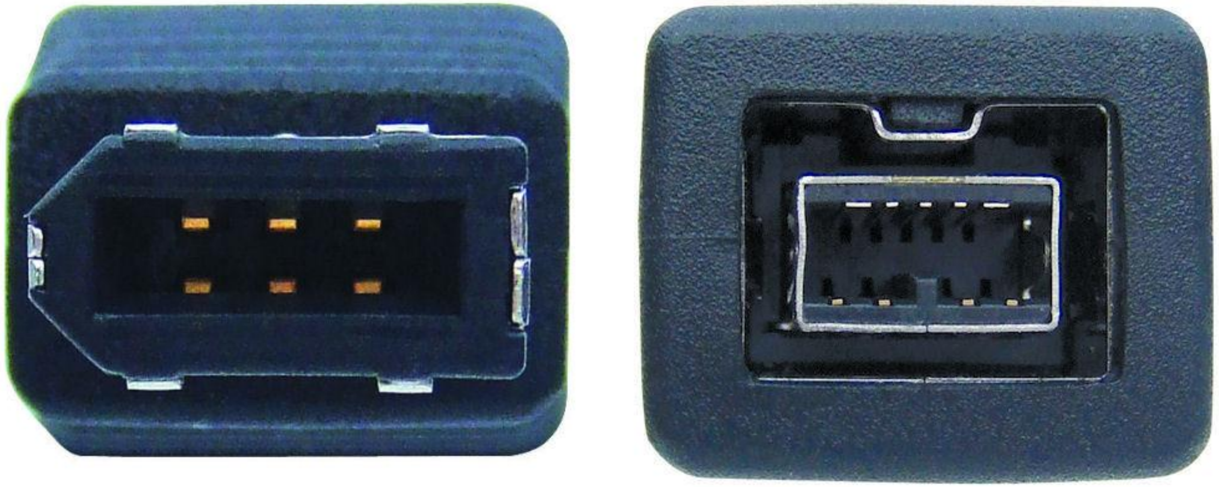
TC7-9-9

The TC7-9-9 is a six foot long, 9p-9p FireWire800 cable.

Compatible With:
T35es-R2, T6es, T8-R2, T9, T35689iu, TD3

TCA7-6-9

The TCA7-6-9 is a compact FireWire cable adapter. This adapter is designed to plug into one end of Tableau's TC7-9-9 FireWire800 cable, thereby adapting the cable for use with 6-pin FireWire ports



Compatible With:

TC7-9-9, T35es-R2, T6es, T8-R2, T9

TC6-8

The TC6-8 is an eight inch long, high-quality, 80-conductor IDE cable with one 40-pin IDE connector at each end. NOTE: When using IDE hard disk adapters such as the Tableau TDA5-ZIF, TDA5-25, and TDA5-18, use the shorter Tableau TC6-2 cable instead. The TC6-2 is 2 inches long but otherwise identical to the TC6-8. Using the shorter TC6-2 when using IDE drive adapters for notebook hard disks will help to ensure data integrity and trouble-free operation.

Compatible With:
T35es-R2, T35u, T35689iu, T35is, TD2u , TD3, TDPX5

SOFTWARE

- Access Data
- Encase Forensic
- And others that are yet to be explored.

Proposed Experiments

S.NO.	TOPIC
Pre-requisites	Operating System File System Understanding
1	Introduction to Hex Editor, Encase Forensics
2	Hard Drive Imaging
3	Comparison of two files for forensic investigation
4	Live RAM Data Dump
5	Live data dump of internet browser (private browsing)
6	Testdisk, Photorec Tool
7	Live Data Collection in Windows
8	Cygwin
9	Live Data Collection in Unix
10	E-mail forensics

EXP 1: INTRODUCTION TO HEX EDITOR, ENCASE FORENSICS

- A hex editor (or binary file editor or byte editor) is a type of computer program that allows for manipulation of the fundamental binary data that constitutes a computer file.
- With a hex editor, a user can see or edit the raw and exact contents of a file, as opposed to the interpretation of the same content that other, higher level application software may associate with the file format.

whereas

- EnCase contains tools for several areas of the digital forensic process acquisition, analysis and reporting. The software also includes a scripting facility called EnScript with various APIs for interacting with evidence.

- **Our Job: To acknowledge students with these required softwares.**

EXP 2: HARD DISK IMAGING

- When a computer is identified as possibly containing electronic evidence, it is imperative to follow a strict set of procedures to ensure a proper (i.e. admissible) extraction of any evidence that may exist on the subject computer. The first thing to remember is the “golden rule of electronic evidence” – never, in any way, modify the original media if at all possible. Thus, before any data analysis occurs, it usually makes sense to create an exact, bit stream copy of the original storage media that exists on the subject computer. A forensic image, is sometimes referred to as a mirror image or ghost image. Mirror imaging or ghost imaging does not always generate a true forensic image. The same is true for cloning a hard drive. A forensic image may include a single or multiple hard drives, floppy disk(s), CD(s), Zip drive(s) or DVD(s), plus many other types of storage media that now exist. Imaging the subject media by making a bit-for-bit copy of all sectors on the media is a well-established process that is commonly performed on the hard drive level, hence often referred to as hard drive imaging, bit stream imaging or forensic imaging.

- **Our Job: To explain the significance of hard disk imaging and how it’s carried out in hostile environment. With the help of FRED, we’ll explore various kinds of hard disk that can be found.**

EXP 3: COMPARISON OF TWO FILES FOR FORENSIC INVESTIGATION

- Compare It! displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with single mouse click or keystroke, and of course you have ability to edit files directly in comparison window. It can make colored printout of differences report, exactly as it's on the screen. It supports regular expressions, so you could easily strip XML tags from file to compare XML with XML or XML with text!? While running on all MS Windows variants, Compare It! can compare merge save text files from DOS, Windows, UNIX, Mac systems. It can create HTML report of your results.

- **Our Job: To let students acknowledge two broad ways of comparing files. First is through Hex Editor and second through fc command in command prompt.**

EXP 4: LIVE RAM DATA DUMP

- 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).
- **Our Job: To explain the significance of RAM, its content and how to take its ram dump in running PC. Fred will perform this task with 3x better speed.**

EXP 5: LIVE DATA DUMP OF INTERNET BROWSER (PRIVATE BROWSING)

- Browser Cache: The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded once in case they're needed again.
- When you first visit a page on this site, the browser downloads the logo into the cache, and then displays it on the page you're viewing. For each additional page you visit, the logo doesn't need to be downloaded again; as long as the same logo is displayed, it's already on your hard disk.
- The cache has a size limit, which you can usually configure. When the cache gets full, the items in it that haven't been used in a while are discarded to make more space.
- **Our Job: To hold an interactive session first about what kind of data they store in web browser and then would continue with dumping of even deleted data. We'll explain how incognito mode of browser is nothing helpful while dumping data.**

Exp 6: Testdisk, Photorec Tool

- TestDisk is OpenSource software and is licensed under the terms of the GNU General Public License (GPL v2+).
- TestDisk is powerful free data recovery software! It was primarily designed to help recover lost partitions and/or make non-booting disks bootable again when these symptoms are caused by faulty software: certain types of viruses or human error (such as accidentally deleting a Partition Table). Partition table recovery using TestDisk is really easy.
- TestDisk can
- Fix partition table, recover deleted partition
- Recover FAT32 boot sector from its backup
- Rebuild FAT12/FAT16/FAT32 boot sector
- Fix FAT tables
- Rebuild NTFS boot sector
- Recover NTFS boot sector from its backup
- Fix MFT using MFT mirror
- Locate ext2/ext3/ext4 Backup SuperBlock
- Undelete files from FAT, exFAT, NTFS and ext2 filesystem
- Copy files from deleted FAT, exFAT, NTFS and ext2/ext3/ext4 partitions.
- **Our Job: To let students know the difference between data recovering using these two renowned software TeskDisk and PhotoRec.**

EXP 7: LIVE DATA COLLECTION IN UNI

- Pre-requisites: Unix Architecture
- **Our Job: This will be the most interesting of all the experiments, since Unix is considered to be safest among all OS (However this is wrong notion). Our purpose is to disprove this notion and compare what other OS can do.**

EXP 8: CYGWIN

- a large collection of GNU and Open Source tools which provide functionality similar to a Linux distribution on Windows.
- a DLL (cygwin1.dll) which provides substantial POSIX API functionality.
- Cygwin is not:
- a way to run native Linux apps on Windows. You must rebuild your application *from source* if you want it to run on Windows.
- a way to magically make native Windows apps aware of UNIX® functionality like signals, ptys, etc. Again, you need to build your apps *from source* if you want to take advantage of Cygwin functionality.
- **Our Job: To *Get that Linux feeling - on Windows***

EXP 9: LIVE DATA COLLECTION IN WINDOWS

- Pre-requisites: Windows Architecture

- **Our Job: This will be the most interesting of all the experiments, since Windows is considered to be worst amongst all OS (Though this is correct !). Our purpose is to verify this notion and compare what other OS can do.**

EXP 10. E-MAIL FORENSICS

- **Our Job: To bring out the loopholes in popular e-mail servicing solutions like Yahoo ! and Gmail !. We will see various ways through which attacker can actually get hold of your inbox.**

References

- https://www.digitalintelligence.com/
- www.google.com/images