Helix3

◎ Team Namaste ◎
Ashish Rajthala, Nirmal Panta, Arjan Regmi

What is cyber forensics?

- Application of computer investigation and analysis techniques to gather evidence suitable for presentation in the court of law
- Goal is to perform structured investigation to find exactly what happened on a computer & who was responsible
- Investigators make a digital copy of the suspected devices' hard drive
- The copy of the hard drive is then analyzed using forensics tools such as Helix3

How to download/install?

- Helix is an e-fense product
- Go to: http://www.e-fense.com/helix/
- Download the helix2009R1.iso file
- Using RUFUS or UnetBootin, create a bootable optical disk or pendrive.

Modes of Helix Operation

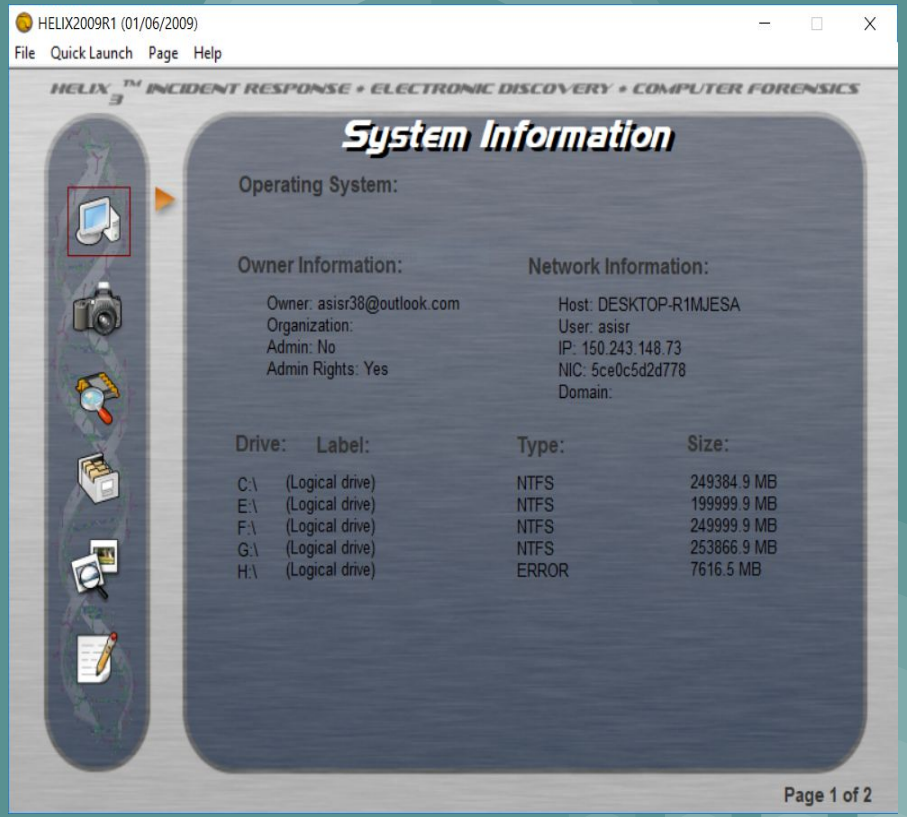
- **Live Response or Windows application:**
  - Runs as a standard windows application
  - It is a portable forensic environment.
  - Includes forensic tools such as System Information, Live Acquisition, Incident Response, scanning Pictures and investigators' report.
- **Linux (Bootable Linux distro with Helix3):**
  - Runs "live" off of CD or USB
  - Analyzes powered off systems
  - Based off of Ubuntu 8.04

What's in it?

Live Response or Windows Application:

Using a live window helix Application is like going through step by step process to see what's going on in the suspects machine.

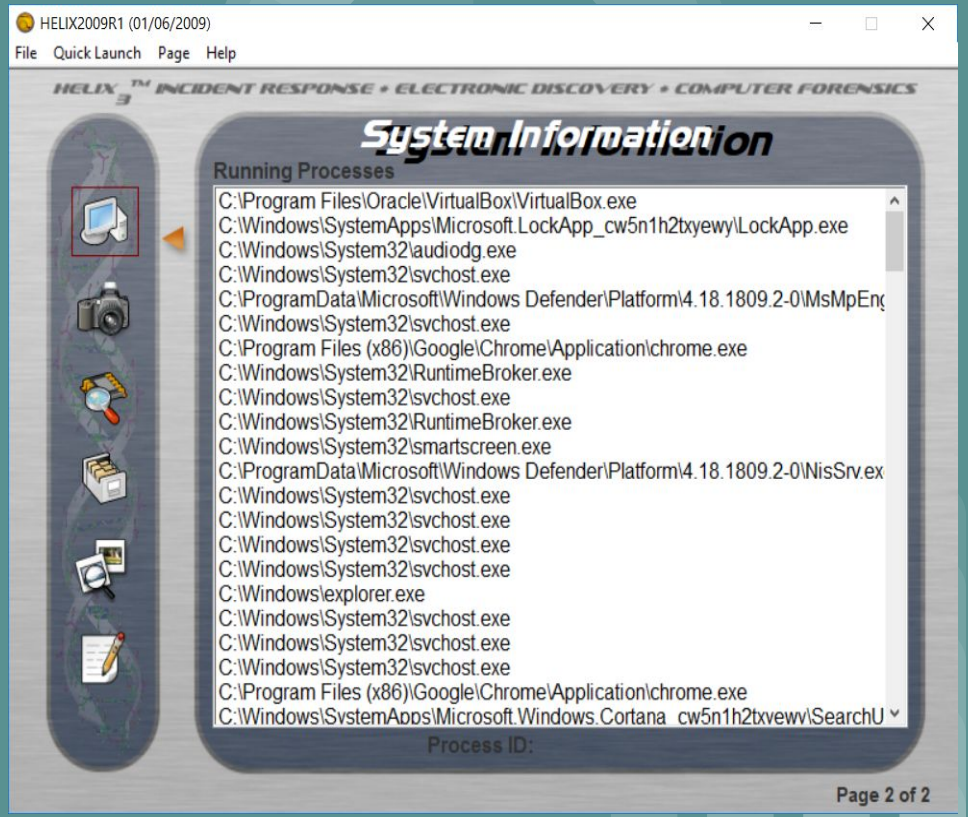
- System Information:
  - Displays basic system information of host device such as username, operation system used, network information including MAC address and IP address of host machine



What's in it?

Live Response or Windows Application(cont.):

- Running Processes:
  - Can see what processes are running on the system
  - Without letting the knowledge of suspect.



What's in it?

Live Response or Windows Application(cont.):

- Live Acquisition:
  - Acquire live image of a system. Two ways of acquisition:

I. DD Utility

(dd) stands for Disk Duplication utility. The dd utility can capture physical memory and drives.

II. FTK Imager:

It is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis is warranted

What's in it?

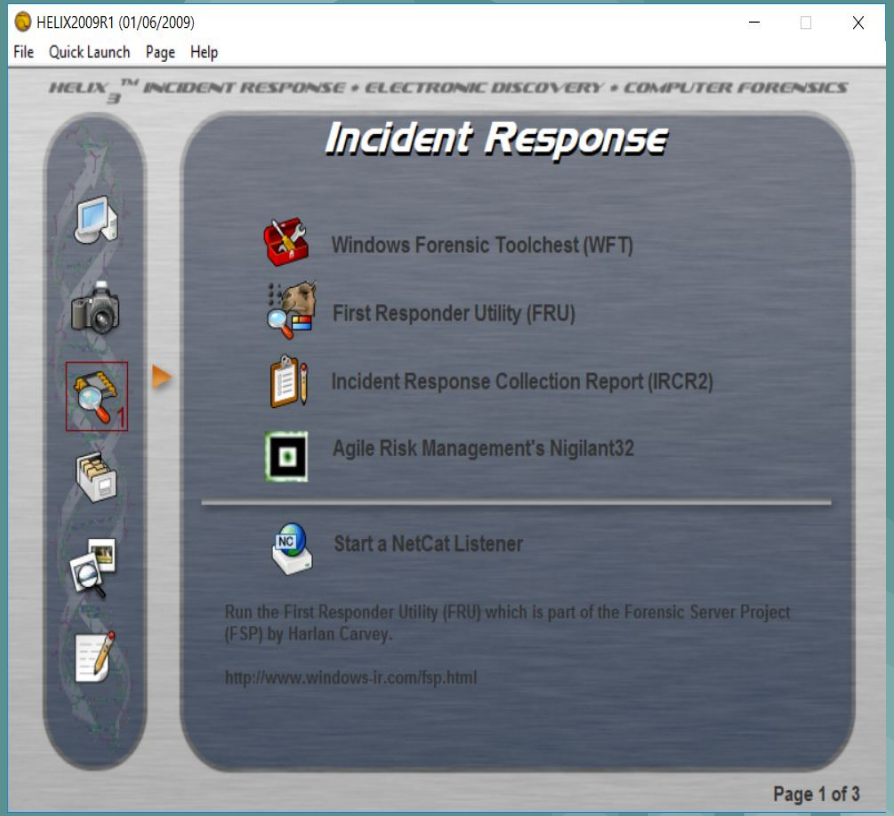
Live Response or Windows Application:

- Incident Response:
  - Windows Forensic toolchest (WFT)

    Collects security relevant information from the system useful for court proceeding.
  - First Responder Utility (FTU)
  - Incident Response Collection Report (IRCR2)

    Tools are oriented towards data collection rather than analysis

  - Agile Risk Management's Nigilant32



What's in it?

Live Response or Windows Application(cont.):

- File Hashing
  - Next feature in incident response includes a simple file hashing interface
  - Picture --->

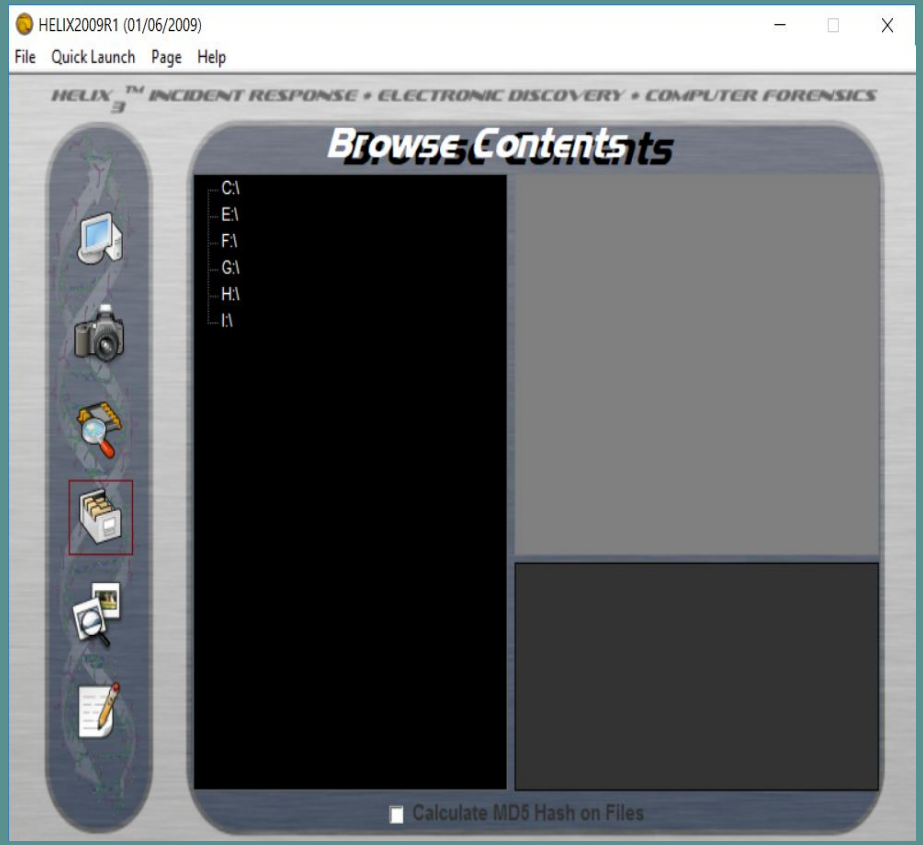
What's in it?

Live Response or Windows Application(cont.):

- More function in Incident Response:
  - PST password Viewer
  - Mail Password Viewer
  - IE history viewer
  - Network Password Viewer

More in the Picture ---->

What's in it?


HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Browse Contents
C:\
E:\
F:\
G:\
H:\
I:\
Calculate MD5 Hash on Files


HELIX2009R1 (01/06/2009)
File Quick Launch Page Help
HELIX3™ INCIDENT RESPONSE • ELECTRONIC DISCOVERY • COMPUTER FORENSICS
Scan For Pictures
Load Folder
Clear All
Enlarge
Decrease

What's in it?

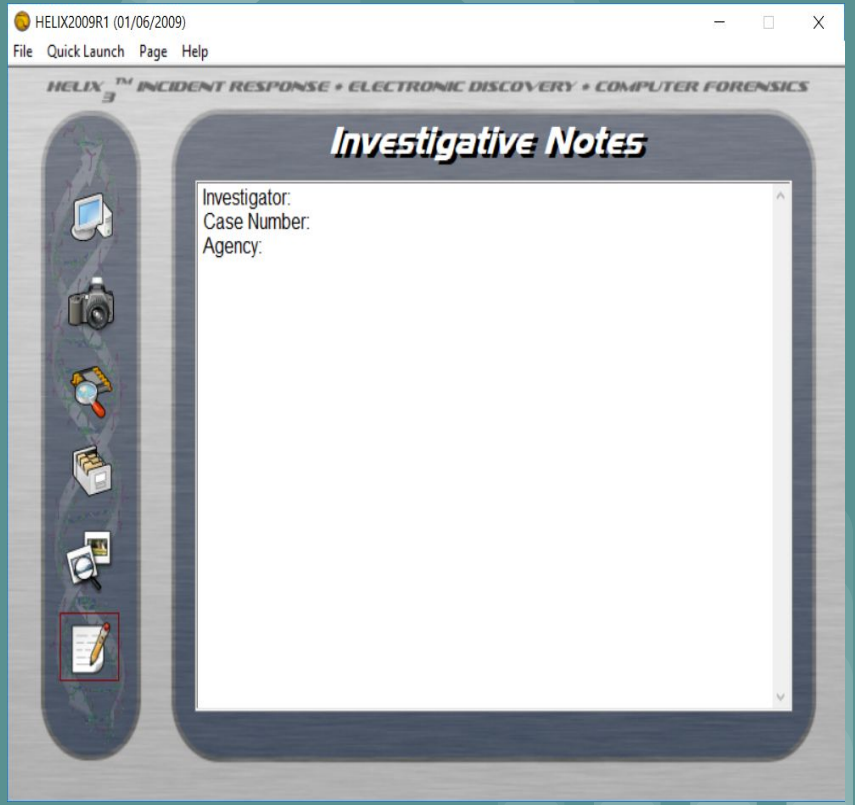
Live Response or Windows Application(cont.):

- **Investigative Notes:**

  Here you write the notes that is required for the investigation.

- Exiting the Helix3

  When you exit the Helix3, the application will prompt you to save the pdf file with all the transaction that took place during the running time of the Helix.



Linux:


HELIX 3
Incident Response, Electronic Discovery, Computer Forensics Live CD
Boot into the Helix Live CD
Check CD for defects
Test memory
Boot from first hard disk
Install Helix
Press F4 to select alternative start-up and installation modes.
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

What's in it?

Linux:

After clicking on the virtual box, if your reboot the suspects machine, it will take you to helix's live linux session.

- Live Session**:** Ubuntu 8.0.4

Some useful tools include:

- **Adepto:** Used for imaging drives, make bit-by-bit copy of the original drive
- **Autopsy:** Forensic tool used for forensic analysis
- **GtkHash:** GUI tool for calculating hashes of the selected file for the purpose of integrity checking.
- **Ophcrack:** Password cracker
- **Wireshark:** ....

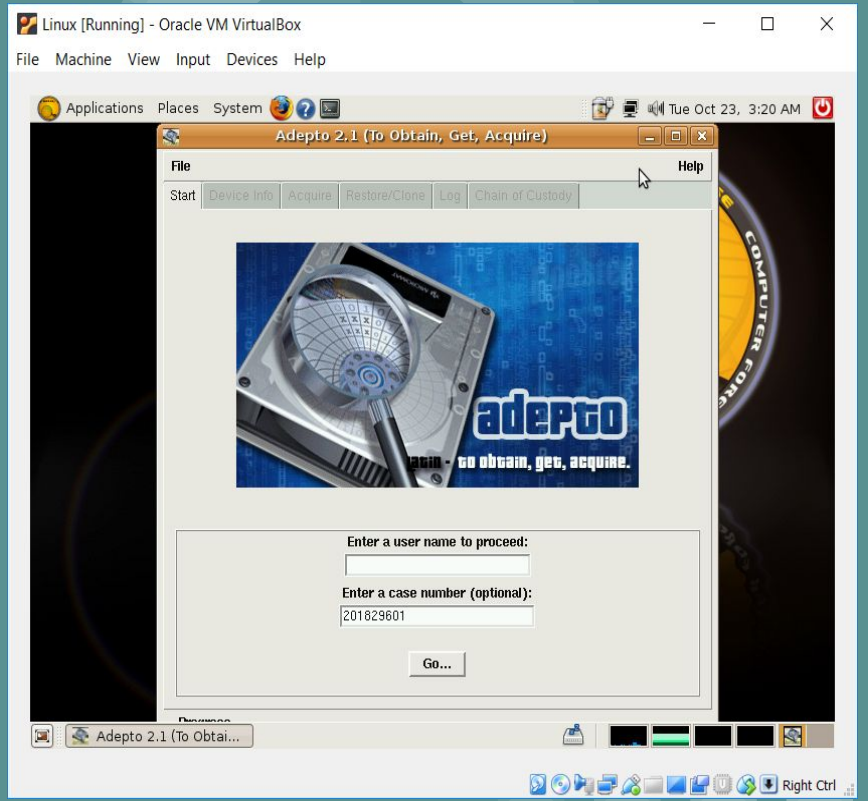
Linux Live Helix3 Forensics and IR applications

Basic Working of tools

- **Adepto:**

Once the user clicks “Go”, the program allows access to several tabs:

- Device Info
  - Info of the device - make, model no., serial number...
- Acquire
  - mention the source and destination along with the hash verification we wish to use and then press Start.
- Restore/Clone
  - Allows users to clone one device to another, Make a forensic copy of the source device
- Log
  - displays a details log of all the actions the user is making.
- Chain of Custody
  - automatically create a chain of custody form based on the device that was imaged.



Advantages of Helix3

- Helix includes dozens of tools for incident response on Windows and Linux Systems.
- It is a Live Linux CD-based forensic tool which does not support auto media access, making it an ideal write-blocker.
- Helix is a live response tool; no imaging or processing has to occur, everything is real-time, so the response time in identifying and quantifying a threat is faster.
- The System Information feature in Helix lets you look at the the suspect's application usage history and system information without the suspect's notice or having to rely on the unreliable Task Manager of the host system.
- It is possible to use Helix to scan and search a user's internet history and saved passwords (for IE) as long as Helix is pre-installed on it.

Disadvantages of Helix3

- As mentioned earlier, the only free version is the 2009 version (old)
- Limited resources on the free version
- No live environment for macOS in the free version
- Application itself feels like beta software and has not been thoroughly tested
- Updates not available anymore, outdated UI and features

Additional Info

- Helix3 Pro
  - Multi-platform Live Environment (Windows, macOS, Linux)
  - Only available through the e-fense forum membership ($239 a year)
  - Includes support from e-fense
- Other relate tools (alternatives to Helix3):
  - CAINE - Computer Aided Investigative Environment
  - Maltego
  - DEFT - Digital Evidence & Forensic toolkit

Wrapping up...

- Technologies such as Helix3 have helped investigate different types of crimes
- Helped monitor and protect corporate and personal computer systems
- Windows side of Helix3 is more popular since most of the corporate world has windows system

Questions?

Helix3 Intro

- Open source forensic analysis toolkit
- Live Linux Security Distributions
- Built to be used in incident response, cyber forensics, e-discovery
- Last free version: 2009