



# HANDS-ON PRACTICALS USING FORENSICS TOOLS



## VIDEO LECTURE

### Task using Forensics Tools



**ProDiscover**

prodiscover

- Suite of products caters to wide range of scenarios handled by law enforcement and corporate internal investigations.
- Finds all the data on a computer disk while protecting evidence and creating evidentiary quality reports for use in legal proceedings.
- Suite is equipped with diagnostic and evidence collection tools for corporate policy compliance investigations and electronic discovery.

1. Create a read-only image of an evidence disk.
2. Jail disks to create and preserve evidence.
3. Instantly capture multiple disks.
4. View locked and encrypted files.
5. MD5 hash of files to verify integrity.
6. Identify known image files.
7. Flexible and powerful full scan engine.
8. Windows, MAC and Linux file systems.
9. Automatically generated evidentiary quality reports.
10. Support's capability for systems table.



**VIDEO LECTURE**

**Deep Information Gathering Tool- Dmitry**



**Deep Information Gathering Tool - Dmitry**

Presented by

**Mr. Sridhar Chandramohan Iyer**

Assistant Professor

Universal College of Engineering, Kaman, Vasai

University of Mumbai



**VIDEO LECTURE**

**Image Metadata Extraction using Imago**



**Image Metadata Extraction using Imago**

---

Presented by

**Mr. Sridhar Chandramohan Iyer**

Assistant Professor


Universal College of Engineering, Kaman, Vasai

University of Mumbai




**VIDEO LECTURE**



**Digital Forensics using EnCase Tool**



**EnCase® Forensic**  
by Guidance Software

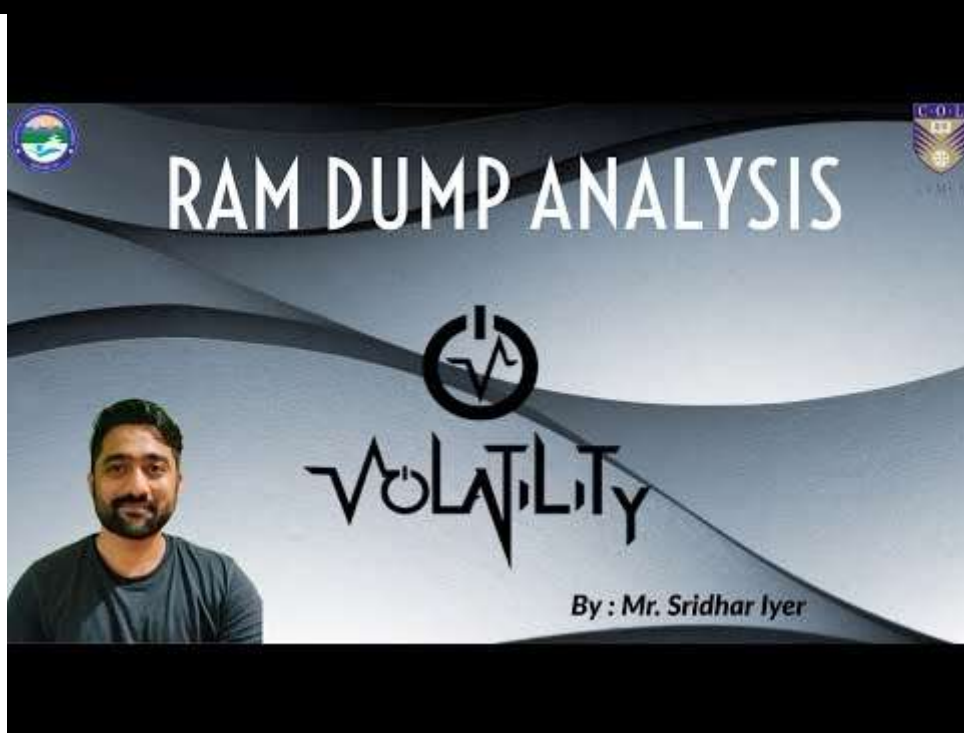


**Rishikesh Ojha**  
Digital Forensics and eDiscovery Expert



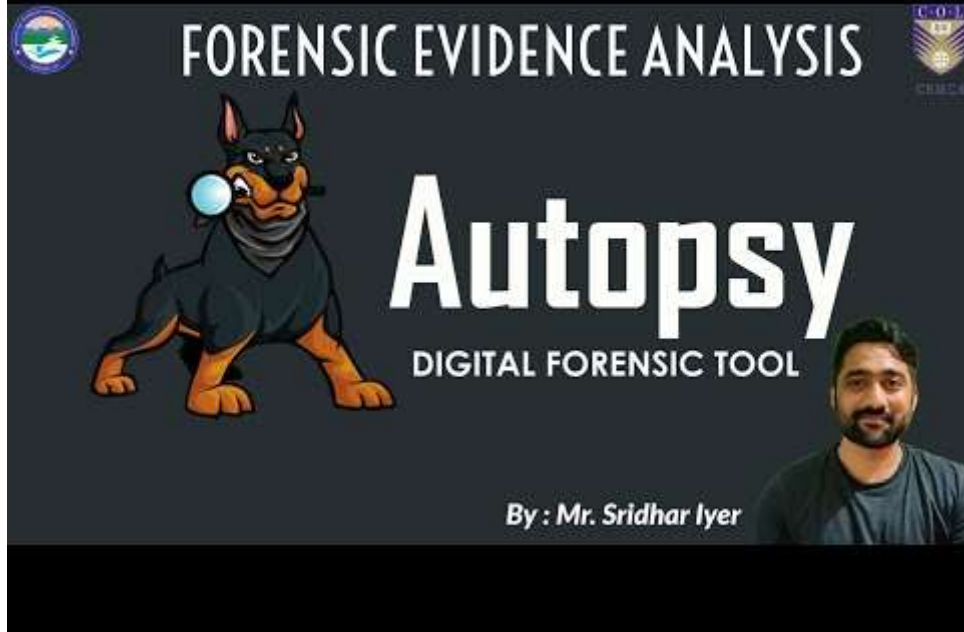
**VIDEO LECTURE**

**RAM Dump Analysis**



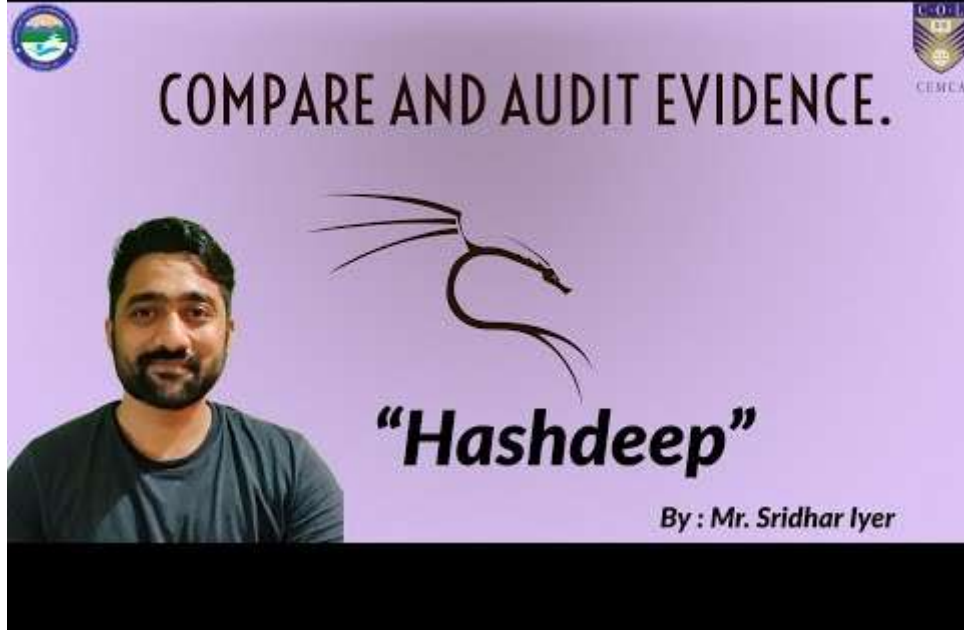
**VIDEO LECTURE**

**Forensic Evidence Analysis using Autopsy**



**VIDEO LECTURE**

**Compare and Audit Evidence using Hashdeep**



The slide features a purple background with a white border. On the left, there is a circular logo with a landscape scene. On the right, there is a shield-shaped logo with the text 'C.O.F.E' and 'CEMCA' below it. The main text 'COMPARE AND AUDIT EVIDENCE.' is centered at the top in a bold, black, sans-serif font. Below this, there is a stylized black line drawing of a dragon's head. The word 'Hashdeep' is written in a large, bold, black, sans-serif font with a slight shadow effect. At the bottom right, the text 'By : Mr. Sridhar Iyer' is written in a smaller, black, sans-serif font. A small portrait of a man with a beard and dark hair is visible on the left side of the slide.

**COMPARE AND AUDIT EVIDENCE.**

**“Hashdeep”**

*By : Mr. Sridhar Iyer*



**VIDEO LECTURE**

**Installation of Kali Linux**

The image is a title card for a video lecture. It features a dark blue background. At the top center, the text "INSTALLATION OF KALI LINUX" is written in a bold, yellow, sans-serif font. To the right of this text is a small logo for "C.O.E. SRMCA". On the left side, there is a portrait of a man with a beard and dark hair, wearing a dark blue t-shirt. To the right of the portrait is a white silhouette of a bird, possibly a phoenix or a similar mythical creature, with its wings spread. Below the bird, the text "INTRODUCTION TO BULK EXTRACTOR" is written in a large, white, sans-serif font. At the bottom center, the text "By : Mr. Sridhar Iyer" is written in a smaller, yellow, sans-serif font. In the top left corner, there is a small circular logo with a globe and some text.

**VIDEO LECTURE**

**Data Carving**



The image is a video lecture cover for "Data Carving Bulk Extractor" by Mr. Sridhar Iyer. It features a dark background with a green dragon logo in the center. The text "DATA CARVING" is prominently displayed at the top in white, and "Bulk Extractor" is written in yellow below it. A portrait of Mr. Sridhar Iyer is on the left, and the author's name "By : Mr. Sridhar Iyer" is at the bottom. Logos for C.O.E and GENCA are in the top corners.

**DATA CARVING**

**Bulk Extractor**

By : Mr. Sridhar Iyer

C.O.E  
GENCA

**VIDEO LECTURE**

**FKT Imager**



**VIDEO LECTURE**

**Live Data Acquisition using FTK Imager**



**VIDEO LECTURE**

**Static Data Acquisition from WINDOWS using FTK Imager**



**VIDEO LECTURE**

**Recovering Evidence for Forensic Images using Scalpel**



**VIDEO LECTURE**

**Computer Forensics using Autopsy and FTK Imager**

**Computer Forensics  
Live Practical  
by using  
Autopsy and FTK Imager**



By: Mr. Rishikesh Ojha



**VIDEO LECTURE**

**Recovering Evidence form Forensics Images using Foremost**



The thumbnail features a central video frame of a man with a beard and dark hair, wearing a blue shirt, against a background of green code. To the left of the video frame is a red circle with a white dollar sign (\$) and a white arrow pointing towards the video. Above the video frame is a red speech bubble containing the text 'HOW TO'. To the right of the video frame, the text 'Recover Evidence from Forensic Images' is displayed in a large, bold, black font. In the top left corner of the thumbnail is a circular logo with a landscape scene. In the top right corner is a shield-shaped logo with the text 'CEMCA' below it.



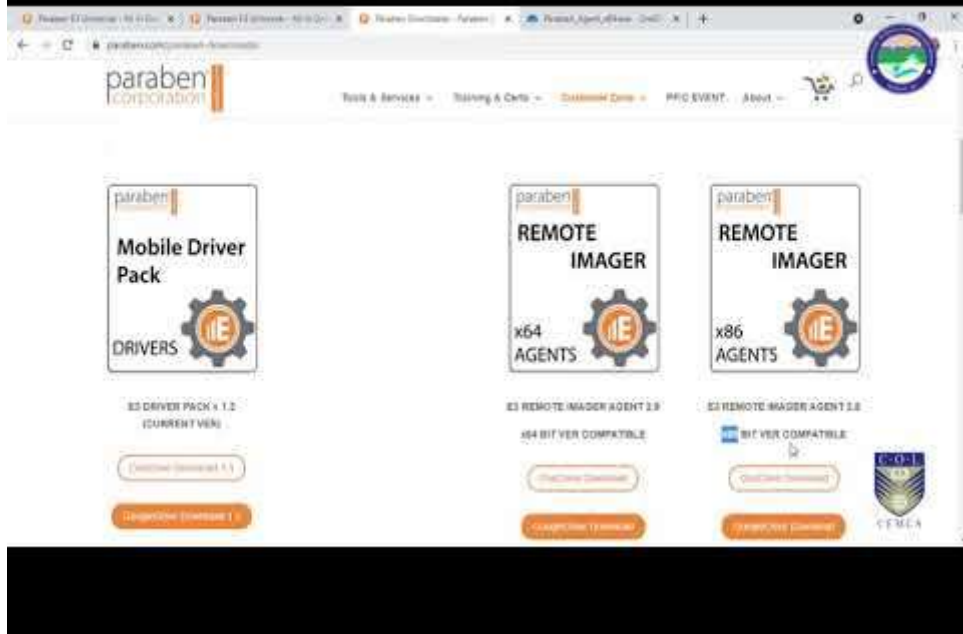
**VIDEO LECTURE**

**Static Data Acquisition Linux OS**



## VIDEO LECTURE

### Remote Imaging using E3 Digital Forensics



The screenshot displays the Paraben Corporation website with three product download cards:

- Mobile Driver Pack**: E3 DRIVER PACK v. 1.2 (CURRENT VER.)  
Download (Current v. 1.2)  
Download (Previous v. 1.1)
- REMOTE IMAGER (x64 AGENTS)**: E3 REMOTE IMAGER AGENT 2.0 (64 BIT VER COMPATIBLE)  
Download (Current v. 2.0)
- REMOTE IMAGER (x86 AGENTS)**: E3 REMOTE IMAGER AGENT 2.0 (32 BIT VER COMPATIBLE)  
Download (Current v. 2.0)

The website header includes the Paraben logo and navigation links: Tools & Services, Training & Certs, Customer Care, PFD EVENT, and About. A shopping cart icon is also visible. The footer features the CEMLA logo.

## **EXPERT PANEL**



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



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



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



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



Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert



Ms. Priyanka Tewari, IT Consultant



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



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



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



This MOOC has been prepared with the support of



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