3 weeks Practical Training Program on

"Cyber Crime and Cyber Forensics"

February 03-21, 2020

3 weeks Practical Training Program with the Cyber P.S./Cell of Ranchi during Jan/Feb 2020 was organized by Department of Computer Science and Technology (DCST) under the school of Natural Sciences of Central University of Jharkhand (CUJ), Ranchi for the M.Tech 2nd Semester students. Students mainly learns about the following things.

➢ Cyber Crime

Cyber Crime is a crime which involves the use of digital technologies in Commission of offence, directed to computing and communication technologies. The activity involves like attacking on Information center Data System, theft, child pornography built images, online transaction fraud, internet sale fraud and also deployment in internet malicious activities such as virus, worm and third party abuse like phishing, email scams etc.

Types of Cyber Crime:-

- Cyber Crime against Person
- Cyber Crime against Property
- Cyber Crime against Nation

➢ Steganography

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

➢ FTK Imager

FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Access Data Forensic Toolkit (FTK) is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence.

Some Important Security Standards and Compliance in Cyber Security

1. HIPPA (Health Insurance Portability And Accountability Act)

2. SOX (Sarbanes Oxley Act3.PCIDSS(Payment Card Industry Data Security Standards)
3. COBIT (Control Objectives for Information Technology)
4. GLBA (Gramm-Leach-Bliley Act)
5. GRC (Governance Risk and Compliance)

3 सप्ताह का प्रैक्टिकल ट्रेनिंग प्रोग्राम

जनवरी / फरवरी 2020 के दौरान रांची के साइबर पीएस / सेल के साथ 3 सप्ताह का प्रैक्टिकल प्रशिक्षण कार्यक्रम सेंट्रल यूनिवर्सिटी ऑफ़ झारखंड के प्राकृतिक विज्ञान स्कूल के कंप्यूटर विज्ञान और प्रौद्योगिकी विभाग के द्वारा आयोजित किया गया था। एम.टेक 2 सेमेस्टर के छात्रों ने मुख्य रूप से निम्नलिखित बातों के बारे में सीखा।

- **साइबर अपराध**

साइबर अपराध एक ऐसा अपराध है जिसमें संगणन और संचार प्रौद्योगिकियों के लिए अपराध आयोग में डिजिटल प्रौद्योगिकियों का उपयोग शामिल है। गतिविधि में सूचना केंद्र डेटा सिस्टम पर हमला, चोरी, बाल पोर्नोग्राफ़ी निर्मित छवियां, ऑनलाइन लेन-देन धोखाधड़ी, इंटरनेट बिक्री धोखाधड़ी और वायरस जैसी इंटरनेट दुर्भावनापूर्ण गतिविधियों में तैनाती और फ़िशिंग, ईमेल स्कैम आदि जैसे दुरुपयोग शामिल हैं।

साइबर अपराध के प्रकार: -

- व्यक्ति के खिलाफ साइबर अपराध
- संपत्ति के खिलाफ साइबर अपराध
- राष्ट्र के खिलाफ साइबर अपराध

- **स्टेग्नोग्राफ़ी**

  स्टेग्नोग्राफ़ी डेटा के भीतर छिपा डेटा है। स्टेग्नोग्राफ़ी एक एन्क्रिप्शन तकनीक है जिसका उपयोग क्रिप्टोग्राफी के साथ-साथ एक अतिरिक्त-सुरक्षित विधि के रूप में किया जा सकता है जिसमें डेटा की सुरक्षा होती है। स्टेग्नोग्राफ़ी तकनीक छवियों, एक वीडियो फ़ाइल या एक ऑडियो फ़ाइल पर लागू की जा सकती है। आमतौर पर, स्टेग्नोग्राफ़ी को हैश मार्किंग सहित वर्णों में लिखा जाता है, लेकिन छवियों के भीतर इसका उपयोग भी आम है। किसी भी दर पर, स्टेग्नोग्राफ़ी अनधिकृत देखने में सहायता के साथ-साथ कॉपीराइट की गई सामग्रियों से सुरक्षा करती है।

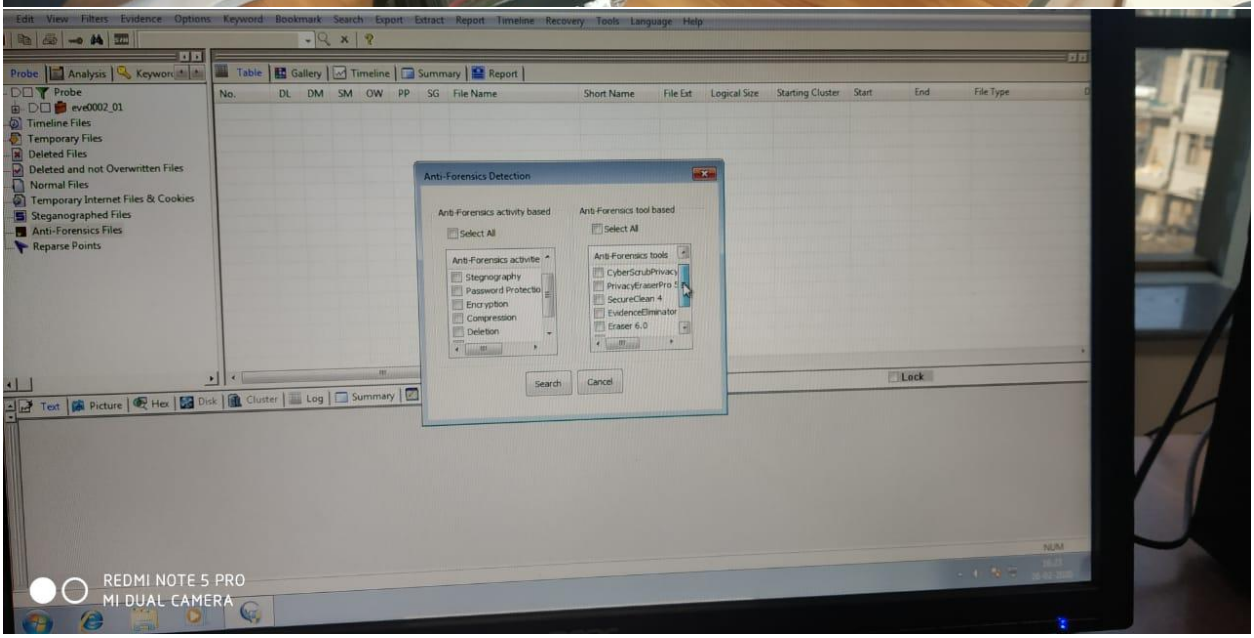
- **एफटीके इमेजर**

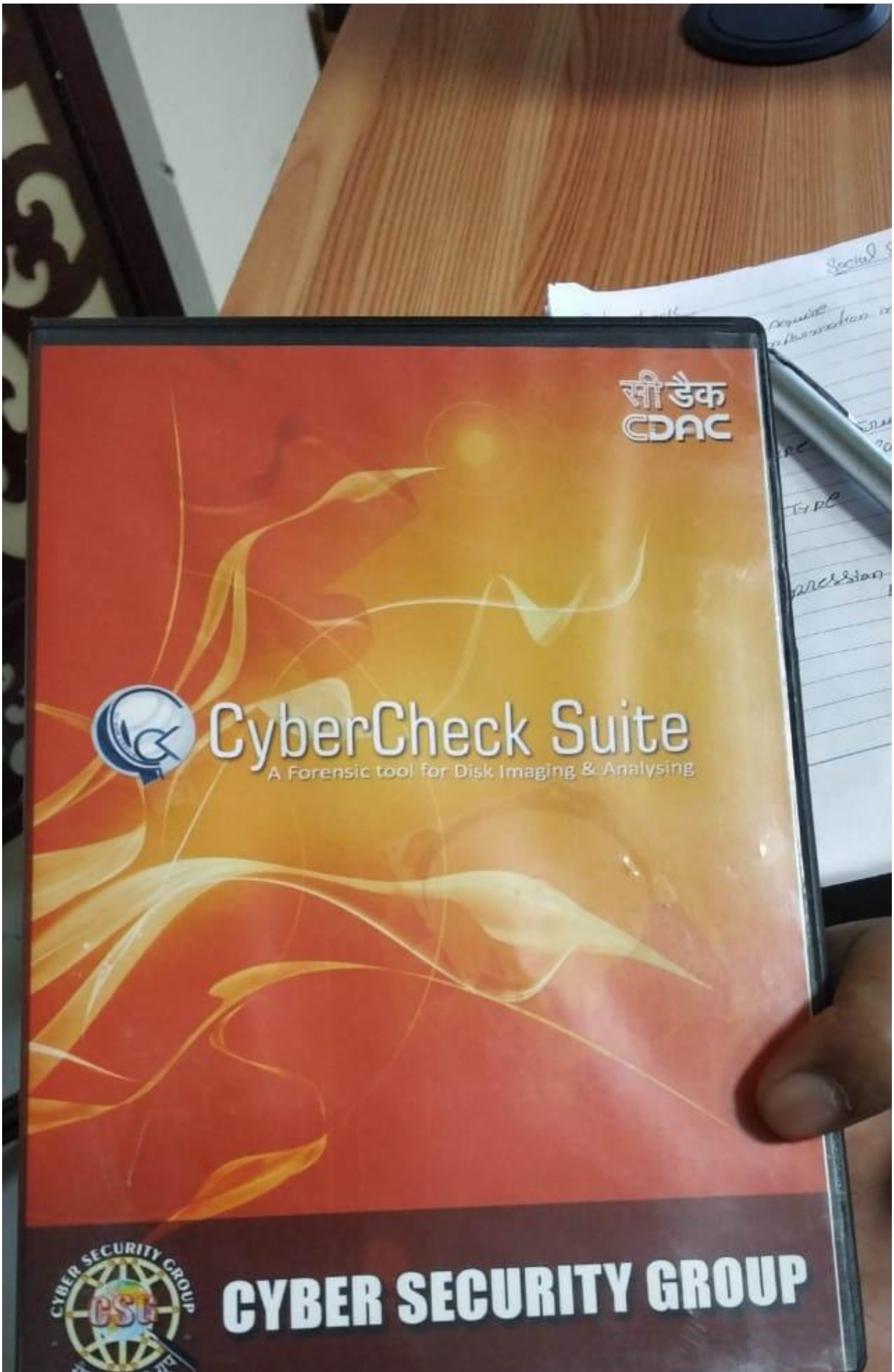
  एफटीके इमेजर एक डेटा पूर्वावलोकन और इमेजिंग उपकरण है जो आपको यह निर्धारित करने के लिए जल्दी से इलेक्ट्रॉनिक साक्ष्य का आकलन करने की अनुमति देता है कि क्या फॉरेंसिक टूल जैसे एक्सेस डेटा फॉरेंसिक टूलकिट (एफटीके) के साथ और विश्लेषण किया जाता है। एफटीके इमेजर मूल सबूतों में बदलाव किए बिना कंप्यूटर डेटा की सही प्रतियां (फोरेंसिक छवियां) भी बना सकता है।

साइबर सुरक्षा में कुछ महत्वपूर्ण सुरक्षा मानक और अनुपालन

1. HIPPA (स्वास्थ्य बीमा पोर्टेबिलिटी और जवाबदेही अधिनियम)
2. एसओएक्स (सरबेंस ऑक्सले एक्ट 3.पीसीआईडीएसएस (भुगतान कार्ड उद्योग डेटा सुरक्षा मानक)
3. COBIT (सूचना प्रौद्योगिकी के लिए नियंत्रण उद्देश्य)
4. GLBA (ग्राम-लीच-ब्लिली एक्ट)
5. जीआरसी (शासन जोखिम और अनुपालन)

REDMI NOTE 5 PRO
MI DUAL CAMERA


Edit View Filters Evidence Options Keyword Bookmark Search Export Extract Report Timeline Recovery Tools Language Help
Probe
Analysis
Probe
eve0002_01
Timeline Files
Temporary Files
Deleted Files
Deleted and not Overwritten Files
Normal Files
Temporary Internet Files & Cookies
Steganographed Files
Anti-Forensics Files
Reparse Points
Table
Gallery
Timeline
Summary
Report
No. DL DM SM OW PP SG File Name Short Name File Ext Logical Size Starting Cluster Start End File Type
Anti-Forensics Detection
Anti-Forensics activity based
Select All
Anti-Forensics activities
Stegnography
Password Protection
Encryption
Compression
Deletion
Anti-Forensics tool based
Select All
Anti-Forensics tools
CyberScrubPrivacy
PrivacyEraserPro 5
SecureClean 4
EvidenceEliminator
Eraser 6.0
Search
Cancel
Lock
Text
Picture
Hex
Disk
Cluster
Log
Summary
REDMI NOTE 5 PRO
MI DUAL CAMERA


सी डैक
CDAC
CyberCheck Suite
A Forensic tool for Disk Imaging & Analysing
CYBER SECURITY GROUP
CSG

REDMI NOTE 5 PRO
MI DUAL CAMERA