Digital Evidence and First Responder Procedure

MODULE 3

Contents

Digital Evidence and First Responder Procedure

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Explain various types of investigations
- Classify techniques of digital forensics
- Understand volatile data
- Discover the importance of volatile data
- List order of volatility of digital evidences

3.2 DIGITAL EVIDENCE

Digital evidence[1] or **electronic evidence** is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required. Some of the popular electronic devices which are potential digital evidence are: HDD, CD/DVD media, backup tapes, USB drive, biometric scanner, digital camera, smart phone, smart card, PDA, etc.

The digital evidence are used to establish a crediable link between the attacker, victim, and the crime scene. Some of the information stored in the victim's system can be a potention digital evidence are IP address, system log-in & remote log-in details, browsing history, log files, emails, images, etc.

3.2.1 Locard's principle[2]

"Wherever a criminal step, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

[1] https://en.wikipedia.org/wiki/Digital_evidence

[2] http://self.gutenberg.org/article/whebn0001722373/locard

Digital evidence is usually not in a format that is directly readable by human. Therefore, it requires some additional steps to convert it into a human readable form in the form of writing. Digital evidences must follow the requirements of the Best Evidence Rule.

VIDEO LECTURE

DIGITAL EVIDENCE

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

BEST EVIDENCE RULE

LOCARD'S PRINCIPLE

3.2.2 Best Evidence Rule[3]

The best evidence rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions:

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.
- The original was destroyed in the normal course of business.
- The original is in possession of a third party who is beyond the court's subpoena power.

This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

3.2.3 Characteristics of Digital Evidence

Following are essential chaterchteristics of a digital evidence:

- **Admissibility:** It must be in confirmity with common law and legislative rules. There must be relationship between the evidence and the fact being proved. Digital evidence

[3] https://www.cccure.org/Documents/HISM/555-558.html

is often ruled inadmissible by courts because it was obtained without authorization. In most jurisdictions a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another.

- **Reliability**: The evidence must be from indisputed origin.
- **Completeness**: The evidence should prove the culprit 's actions and help to reach a conclusion.
- **Convincing to Judges:** The evidence must me convincing and understandable by the judges.
- **Authentication**: The evidence must be real and related to the incident. Courts largely concerned themselves with the reliability of such digital evidence. The investigator must be able to prove to the authenticity of the digital evidence by explaining:
    - the reliability of the computer equipment.
    - the manner in which the basic data was initially entered.
    - the measures taken to ensure the accuracy of the data as entered.
    - the method of storing the data and the precautions taken to prevent its loss.
    - the reliability of the computer programs used to process the data, and
    - the measures taken to verify the accuracy of the program.

3.2.4 Stages in Digital Evidence Investigation Process[4]

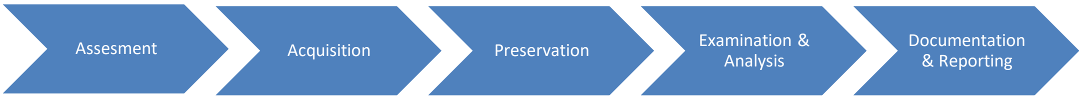


Figure 1: Stages in digital evidence investigation process

- **Assesment:** It is a key point of an investigation where the potentially relevant sources of information are identified. Without this stage the chance to preserve and collect relevant material can be lost. This stage could also inform other activities including gathering information about possible passwords and attempts to attribute the sources to individuals as ownership of a device or a document can be a point of contention later on. In this phase the investigator make assesment of the situation anc consider many factor for making an assesment like whether the investigation is to be perforemed internally or an external agency is to be involved; Whether a search warrent is required. Also, some pre-search investigation need to be performed like gathering information about the infrastructure and assets of the company; gathering information about the employees who are directly or indirectly involved with the case; gathering information

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf

about the security incident team and their key skills, etc. Also the investigator need to prepare and check the forensic investigation toolkit to conduct the investigation. He also needs to brief the investigating team about the search strategy; guidelines to be followed while investigation for eg. maintaing the logs of the events, chain of evidence and chain of custody. Chain of evidence is the process of documenting each and every step carried out during the investigation process to prove the authenticity of the digital evidence in the court.

VIDEO LECTURE

- **Acquisition:** It is a process of gathering the data from wherever it resides. The most common collection approach is to create an image of a target device which can then be examined without altering the original exhibit. In a wider sense, this could also apply to aspects such as requesting and receiving communications data. Cloud storage is an increasing concern and whilst the forensic recovery of files stored remotely is possible, the subsequent analysis may require detailed knowledge of the application used. Complications can also arise from the data being held in a different jurisdiction. The goal of the investigator in this phase is to acquire the evidence in a forensically sound manner so that it is acepted by court of law. It is good practice to record the physical attributes of every digital media like serial number, make, model, IP address and MAC address in case of network devices like NIC card, etc. and label them clearly so that they can easily be identified in later course of action. It is also a sound practice to gather information regaring the user login, password, etc. from the users and system administrators. Remember to use forencially clean storage device to store the evidence. For making copy of the digital evicende, use bit-stream copy option, which acquire bit-by-bit image of the original evidence and can be considered as equalivent to original for the purpose of investigaion. Don’t forget to calculate checksum or hash value of the on original copy and duplicate copy. The same value of checksum and hash value will gurentee both the copies are technically same for the purpose of investigation. It is important to note that logs from the servers, fairewalls, routers, and stand alone devices should also be recorded. Precautions regaring static electricty and magnetic fields should be taken while acquiring the digital evidence as it may alter data present in the digital devices. Therefore anti-static bags are used to store the digital evidence. The investigator must thoroughly examine the situation and if deemed essestial, a futher search warrent amy be required to search third party data carriers like ISP. After acqusation, the chain of custody, which the record of history of the custody of the evidence is prepared and recorded.

- **Preservation:** Preserving the digital evidence is as important as acquiring it and proper case must be taken to preserve the evidence so that data stored in digital storage devices can be used to investigate the case. It is advisable to take the photograph of the computer, cabling and the devices that are attached to the victim’s computer, which are as important as victim’s computer. Also label the seized cables along with the media. It is important to note that only forensically clean storage devices should be used to store the logs and other important digital information from the victim’s system. Avoid dust, scratch, and exposure to magnetic or electric field by using antistatic bags. Care must also be taken to save the digital evidence from exposure to wireless radiations by storing them in wireless holdbags. One must avoid the use of USB drive or fireware drive as they change the state of the system. Intentional or accidental modification of data during the acquisition and preservation stage should be avoided and in case, it occurs, record the changes made in the system. Make the storage devices write-protect in order to accidentally overwrite the data. After bringing the digital media to the forensics lab, proper chain of custody should be maintain and these evidences should be stored in a physically safe location with access control facility. Also enough duplicate copies of the media should be made to carry out the investigation. *NEVER USE ORIGINAL MEDIA FOR CARRING OUT INVESTIGATION*.
- **Examination and Analysis:** The purpose of examination and analysis process is to make sense of the diverse digital data collected. A range of tools and techniques are used for this in an effort to ensure that as much data as possible is available for review. A lot of this data is of no relevance to the investigation but it may take considerable effort to get a good understanding of the relevance of material and to present it in an intelligible form. This data is examined and analysed to draw meaningful conclusions for the case. The first and the foremost thing to be kept in mind is the examination should be done be a trained person as mishandling of digital devices may corrupt the data. Examination requires the data to be extracted to the testbed for analysis. While examining, the goal of the investigator is to find out if files, folders, emails, partitions are deleted and use recovery tools to restore them. Also, check if traces of data wiping software is present in the system so that special strategies could be use to recover data. If the files and documents are password protected then check whether the password for the same are available, else use password cracking software to crack the password and

gain access to the files. The second important task after examination is analysis. It is the process of putting the different pieces of evidence together to allow conclusions to be drawn and ideas tested. Some units have dedicated analytical support available which is a useful resource but many investigators don not have routine access to analysts so it can be helpful for the investigator to be able to conduct their own analysis. The primary information is gathered based on the interviews conducted with the witnesses at the crime site which is then used to frame the keywords to search the relevant document, files, etc. for investigation. The photographs, paper documents seized during the raid, etc are useful for analysis. The Investigator look for document properties, file signatures, browser history, chat history, emails, printer spools, cache files, registry files, timeframe, ownership information, etc. to find clues and missing link. Hash values are compared to find weather a duplicate or multiple copies of the file exist. If required, use decrypting software to decrypt the files if they are encrypted. The most important point in the analysis process is to keep the log of all the steps carried out during the examination & analysis phase including the details of keywords used, the list of search results returned using these keywords, searching methodology used while carrying out investigation, etc.

- **Documentation and Reporting:** The examination and analysis can be conducted at a highly technical level but the information will ultimately need presenting to other individuals, either elsewhere in the investigation or the legal process, who are not so familiar with the detailed processes used and are more concerned with the usefulness of the information provided. Therefore documentation and reporting is a crucial part of the digital evidence investigation process. During this phase detailed report is perfored which includes all the information related to the case like details of OS, software, versions, patched installed in the machine and detailed note about the action taken during the forensic investigations along with the keywords seaches, logs, cache, etc . It also document any point that is contrary to the rules or to that which is normal or established. It also consists of the details of data analysing and the findings of the investigator.

3.3 FIRST RESPONDER TOOLKIT

The first responder is the person who first accesses the victim's computer. He must be prepared well to collect the evidences for the crime scene in a manner that is accepted by the court. Therefore, availability of trusted digital forensics toolkit is necessary for the first responder. Some of the important steps in preparing first responder's toolkit are:

1. Create forensics tool testbed.
2. Document the forensics tool testbed.
3. Document the summery of the forensics tools.
4. Test the tools.
5.

VIDEO LECTURE

Create Forensic Tool Testbed

The testbed should be created from the trusted source and functionality of the testbed should be checked in advance before using them in the field.

The above four steps are described in details in the following section.

1. **Create forensic tool testbed-** The testbed should be created from the trusted source and functionality of the testbed should be checked in advance before using them in the field. Some of the guidelines are:
    a. Identify the appropriate OS type your organization is using, based on which the testbed is created. An organization may have verity of OS deployed in its network. For eg. it may have Linux based servers and Windows and Mac based PC/Laptop. In that case, one has to create multiple testbeds for each OS type.
    b. Disinfect the testbed from the availability of any data on the machine. Preferably use a new/fresh machine. In case, a new machine is not available use wiping tools to wipe out any data from the machine.
    c. Install OS and all the necessary software to conduct the forensics investigation.
    d. Ensure that the OS and all the programmes installed in the testbed are updated to latest version. If any patch is required for the successful operation of the system, the same should also be installed.
    e. Compute Hash to ensure the integrity of the file system.
2. **Document the forensics tool testbed:** It includes the following
    a. Name, type and version of OS
    b. Details of the types of various applications/software installed in the testbed along with the details of the upgrades and patches.
    c. Details of various types of hardware installed in the testbed.
    d. Details pertaining to hash and checksum of the testbed.

3. **Document the summery of the forensics tools:** For every tool that is acquired for the testbed, the following information is documented for easy reference and record.
    a. Details about the source from where the software was brought. In case it's a freeware, mention the site/source from where the tool was downloaded.
    b. Detailed description about the purpose, working and compatibility of the tool with OS and other software.
    c. Details of tool dependencies and the system effects which include the details about the required system access levels by the user to run a tool and the details of shared libraries.
4. **Test the tools:** Now the tools selected and installed are tested in the testbed and its performance and output is examined.

3.3.1 Some Common Mistakes First Responder should avoid

- Do not shut-off or reboot the machine. This will erase all the valuable data present in the volatile devices.
- Do not assume that any parts of the victim/suspicious computer are reliable. Take precautions and follow procedures otherwise may accidently trigger malware which will effect/change/delete volatile data.

3.4 ISSUES FACING COMPUTER FORENSICS

The issues facing computer forensics examiners can be broken down into three broad categories: technical, legal and administrative[5].

3.4.1 Technical issues

a. Encryption – Encrypted data can be impossible to view without the correct key or password. Examiners should consider that the key or password may be stored elsewhere on the computer or on another computer which the suspect has had access to. It could also reside in the volatile memory of a computer (known as RAM) which is usually lost on computer shut-down; another reason to consider using live acquisition techniques, as outlined above.

b. Increasing storage space – Storage media hold ever greater amounts of data, which for the examiner means that their analysis computers need to have sufficient processing power and available storage capacity to efficiently deal with searching and analysing large amounts of data.

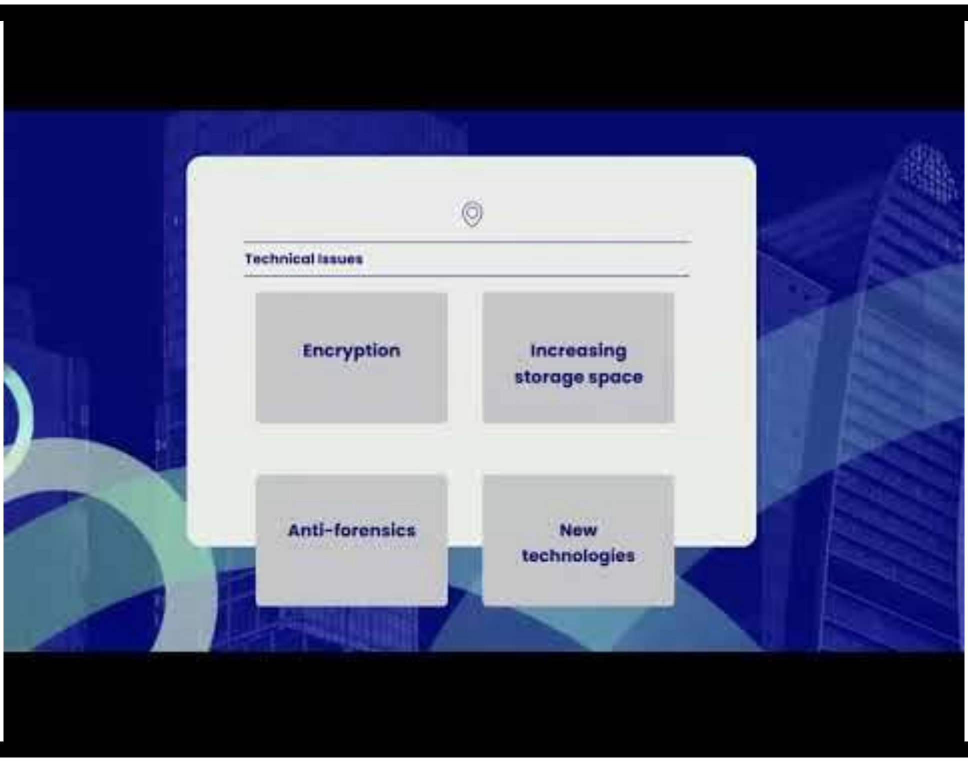
c. New technologies – Computing is a continually evolving field, with new hardware, software and operating systems emerging constantly. No single computer forensic examiner can be an expert on all areas, though they may frequently be expected to analyse something which they haven't previously encountered. In order to deal with this situation, the examiner should be prepared and able to test and experiment with the behaviour of new technologies. Networking and sharing knowledge with other computer forensic examiners is very useful in this respect as it's likely someone else has already come across the same issue.

d. Anti-forensics – Anti-forensics is the practice of attempting to thwart computer forensic analysis. This may include encryption, the over-writing of data to make it unrecoverable, the

[5] https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

modification of files’ metadata and file obfuscation (disguising files). As with encryption, the evidence that such methods have been used may be stored elsewhere on the computer or on another computer which the suspect has had access to. In our experience, it is very rare to see anti-forensics tools used correctly and frequently enough to totally obscure either their presence or the presence of the evidence that they were used to hide.

VIDEO LECTURE



Technical issues

Encryption

Increasing storage space

Anti-forensics

New technologies

3.4.2 Legal issues

Legal issues may confuse or distract from a computer examiner’s findings. An example here would be the ‘Trojan Defence’. A Trojan is a piece of computer code disguised as something benign but which carries a hidden and malicious purpose. A lawyer may be able to argue that actions on a computer were not carried out by a user but were automated by a Trojan without the user’s knowledge; such a Trojan Defence has been successfully used even when no trace of a Trojan or other malicious code was found on the suspect’s computer. In such cases, a competent opposing lawyer, supplied with evidence from a competent computer forensic analyst, should be able to dismiss such an argument. A good examiner will have identified and addressed possible arguments from the “opposition” while carrying out the analysis and in writing their report.

3.4.3 Administrative issues

a. Accepted standards – There are a plethora of standards and guidelines in computer forensics, few of which appear to be universally accepted. The reasons for this include: standard-setting bodies being tied to particular legislations; standards being aimed either at law enforcement or commercial forensics but not at both; the authors of such standards not being accepted by their peers; or high joining fees for professional bodies dissuading practitioners from participating.

b. Fit to practice – In many jurisdictions there is no qualifying body to check the competence and integrity of computer forensics professionals. In such cases anyone may present themselves as a computer forensic expert, which may result in computer forensic examinations of questionable quality and a negative view of the profession as a whole.

3.7 SUMMARY

1. Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.
2. The digital evidences are used to establish a crediable link between the attacker, victim, and the crime scene.
3. Digital evidence is usually not in a format that is directly readable my human. Therefore it requires some additional steps to convert it into a human readable form in the form of writing.
4. There must be relationship between the evidence and the fact being proved.
5. The evidence must be from indisputed origin.
6. The evidence must be real and related to the incident.
7. Assessment is a key point of an investigation where the potentially relevant sources of information are identified.
8. Chain of evidence is the process of documenting each and every step carried out during the investigation process to prove the authenticity of the digital evidence in the court.
9. For making copy of the digital evicende, use bit-stream copy option, which acquire bit-by-bit image of the original evidence and can be considered as equalivent to original for the purpose of investigaion.

3.8 CHECK YOUR PROGRESS

1. Fill in the blanks

i. Digital evidences must follow the requirements of the ______________.

ii. ______________ are used to search the relevant files and documents from the digital evidence.

iii. ______________ is the practice of attempting to thwart computer forensic analysis.

iv. A ______________ is a piece of computer code disguised as something benign but which carries a hidden and malicious purpose.

v. ______________ investigation is instigated as a response to a network intrusion.

2. State True or False

i. Digital evidence is often ruled inadmissible by courts because it was obtained without authorization.
ii. The evidence must me convincing and it is not necessary that it should be understandable by the judges.
iii. Any storeage device can be used for storing the digital evidences.
iv. USB memory is a preferred way to store the logs and other information from the victim's computer.

3.9 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks

i. Best Evidence Rule.
ii. Keywords
iii. Antiforensics
iv. Trojan
v. Intrusion

2. True or False

1. True
2. False
3. False
4. False
5. True

3.10 FURTHER READING

Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified ExaminorStudy Guide.* Wiley Publishing Inc.

Computer Forensics: Investigation Procedures and Response. EC-Council Press.

Cowen, D. (2013). *Computer Forensics: A Beginners Guide.*

ENISA, & Anderson, P. (2014). *Electronic evidence - a basic guide for First Responders.* European Union Agency for Network and Information Security.

Godbole, N., & Belapure, S. (2011). *Cyber Security (with CD): Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.* Wiley.

Kent, K., Chevalie, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* Special Publication 800-86, National Institute of Standard and Technology, U.S. Department of Commerce.

Mukasey, M. B., Sedgwick, J. L., & Hagy, D. W. (2008). *Electronic Crime Scene Investigation:A Guide for First Responders Second Edition.* Special report, National Institute of Justice .

Nelson. (2013). *Guide to Computer Forensics and Investigations.*

Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations.* Cengage Learning.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic.* CERT Training and Education.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders Guide to Computer Forensics.*

Schneier, B. (1994). *Applied Cryptography.* Wiley.

Vacca, J. (2009). *Computer Forensics: Computer Crime Scene Investigation.*

Wolfe, H. B. (2007). Electronic Forensics: A Case for First Responders. *19th Annual FIRST Conference on Computer Security Incident Handling.* Spain.

3.11 MODEL QUESTIONS

1. What is digital evidence? What is its role in the investigation process? Give examples of some common digital evidences.
2. State Locard's Principle.
3. What is best evidence rule? Under what circumstances the duplicate copy of the digital evidence is admissible for lawful purposes?
4. What are the essential characteristics of digital evidence?
5. How the authenticity of the digital evidence can be proved?
6. Explain the digital evidence investigation process in detail.
7. What is chain of evidence and chain of custody? Explain.
8. What is first responder's toolkit? What are the steps for preparing first responder's toolkit.

REFERENCES, ARTICLE SOURCE & CONTRIBUTORS

Digital evidence. (2015, Aug. 20). Retrieved Oct. 11, 2015, from Wikipedia: https://en.wikipedia.org/wiki/Digital_evidence

Introduction to computer forensics. (n.d.). Retrieved Oct. 11, 2015, from forensic control: https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

Krause, M., & Tipton, H. F. (Eds.). (1993). *Handbook of Information Security Management.* AUERBACH.

Lawton, D., Stacey, R., & Dodd, G. (2014). *eDiscovery in digital forensic investigation.* CAST publication number 32/14 available under the Open Government Licence v3.0 https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/.

Locard's Exchange Principle. (2005, April 10). Retrieved Oct. 11, 2015, from Project Gutenberg Self-Publishing Press: http://self.gutenberg.org/article/whebn0001722373/locard

Morton, T. (2013, Sep. 13). *Types of investigations.* Retrieved Oct. 11, 2015, from Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types

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, Maharastra

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

C·O·L

CEMCA