Education course
“Cybercrime investigation”

+7 (495) 984 33 64, info@group-ib.com, group-ib.com

We are glad to suggest you the education course “Cybercrime investigation” from digital forensics experts of Group-IB.

You will get skills in:

- Computer security incident response
- Collecting and documenting evidence
- Investigation of different types of digital evidence
- Data recovery
- Reverse engineering
- Preventing computer security incidents or minimizing the risk of them.

The uniqueness of the course is that you can create your own one by combining different trainings depending of you interest, challenges and skills.

Course contents

Service deliverables

All trainings in the course are offered in English. The trainings are designed to include both theoretical and practical classes (labs). Attendees are provided with all required training materials. Upon completion of the course, all attendees will be able to pass a certification program to validate their knowledge on the course subjects.

Overview

The course will give attendees the necessary skills to identify the type of attack, to find out an intruder’s footprints, to properly collect evidence to prosecute and to conduct deep analysis of computer information during an expertise. Now the battlefield starts in the technical realm, which ties into most every facet of modern day life. If you or your organization requires the knowledge or skills to identify, track, and prosecute the cybercriminal, then this is the course for you.

What are the advantages of our course

The course program is designed so that every new unit of information is accompanied by the practical work, that allows attendees to assimilate the new material better and gain the skills of its use in their labor activity. The detailed group analysis of the obtained solutions with the involvement of the teacher let attendees to bring out their mistakes and avoid these mistakes in the future.

At the final session, the participants have an opportunity to choose the real business case which maximally represents the specifics of their work, or to provide their own one, in agreement with the teacher.

Who should attend

Incident Response Team Members

Experienced Digital Forensic Analysts

Red Team Members, Penetration Testers, and Exploit Developers

Law enforcement officers, federal agents, or detectives

Forensics Investigators

Attendees group

It is recommended to create a group for the course from 4 to 10 attendees.

Course duration

The duration of the course depends on the set of trainings.

The duration of each training is provided with its description below.

Prerequisites

No specific prerequisites are required for this course, but knowledge of technical terms is beneficial and will facilitate participation in class discussions.

Attendees will benefit from having some experience with Windows, Linux, Mac OS X and different filesystems.

Trainers qualification

Sergei Nikitin is a practitioner in computer forensics. He is the Deputy Chief of Laboratory of Computer Forensics in Group-IB and has the certificate of GIAC GCFA.

Sergey has a great experience in conducting of forensic expertise, in incident response and participation in law enforcement activities.

He is an author of some publications and education courses, the permanent commentator of hi-tech news in mass media.

He has more than 3 years of experience in the field of trainings and more than 5 years in the field of digital forensics.

Matveeva Vesta is a practitioner in computer forensics. She is a senior computer forensics expert in Group-IB.

Vesta has a great experience in conducting of forensic expertise, in incident response and participation in law enforcement activities.

She is an author of many articles and education courses, techniques of conducting computer expertise and recommendations for information security.

She has more than 3 years of experience in the field of trainings and more than 4 years in the field of digital forensics.

Artemov Artem is a practitioner in computer forensics. He is a senior computer forensics expert in Group-IB.

Artem has a great experience in conducting of forensic expertise, in incident response and participation in law enforcement activities.

He is the permanent commentator of hi-tech news in mass media.

He has more than 4 years of experience in the field of trainings and more than 8 years in the field of digital forensics.

Course trainings

Training 1. Computer Security Incident response team (CSIRT) management

Duration: 4 hours

- Creating of CSIRT based on the goals, objectives and possible digital evidence
- CSIRT members responsibilities
- Collaboration of CSIRT with law enforcement
- Developing incident handling capabilities
- Recommended tools and methods for collecting evidence
- Collecting and documenting evidence
- Creating copies of data from different sources
- Collecting volatile data: memory, traffic, live data of running computer
- Identification of countermeasures: encryption, steganography, remote storage, etc.
- Collecting data from a mobile phone: wireless network isolation, lock bypassing, prevention of remote control and destruction

Training 2. Computer forensics of Windows operating system

Duration: 8 hours

- Computer forensics fundamentals
- Prerequisites for successful cybercrime investigation
- Collecting evidence in Windows operating system
- Recommended Windows tools for forensic data duplication
- Windows artefacts
- Investigation of network connections and creating timeline
- Investigation of the incident with internet banking fraud
- Practical classes

Training 3. Computer forensics of Linux operating system

Duration: 8 hours

- Computer forensics fundamentals
- Prerequisites for successful cybercrime investigation
- Collecting evidence in Linux operating system
- Recommended Linux tools for forensic data duplication
- Linux artefacts
- Investigation of network connections and creating timeline
- Investigation of the incident with web server hacking
- Practical classes

Training 4. Computer forensics of Mac OS X operating system

Duration: 8 hours

- Computer forensics fundamentals
- Prerequisites for successful cybercrime investigation
- Collecting evidence in Mac OS X operating system
- Recommended Mac OS X tools for forensic data duplication
- Mac OS X artefacts
- Investigation of network connections and creating timeline
- Investigation of the incident with compromise of sensitive data and mail history. Analysis of e-mail fabrication.
- Practical classes

Training 5. Memory forensics

Duration: 4 hours

- Memory structure depending on the architecture
- Analysis of Windows memory dumps
- Analysis of Linux memory dumps
- Malware in memory dumps
- Forensic artifacts from memory dump
- Practical classes

Training 6. Network Forensics

Duration: 4 hours

- Topologies of computer networks, protocol stacks, hardware types and types of network addressing
- Forensic analysis of network protocols: HTTP, NTP, FTP, SMTP, wireless protocols
- Methods of creating traffic copies depending on the device
- Forensic reconstruction of data flows in traffic dumps
- Forensic analysis of web proxy servers
- Forensic analysis of HTTP servers
- Forensic analysis of firewalls and IDS/IPS
- Practical classes

Training 7. Reverse engineering

Duration: 8 hours

- Malware dynamic analysis
- Malware static analysis
- Filesystem modification during malware execution
- Windows registry modification during malware execution
- Analysis of malware network connections and sending data
- Reverse engineering of modern malware with anti debugging and obfuscation techniques
- Practical classes

Training 8. Data recovery

Duration: 4 hours

- HDD structure
- Filesystems structure: NTFS, FAT32, ext3/ext4
- Data recovery from damaged HDD
- Recovery of deleted files and damaged/deleted partitions
- Data recovery from RAID
- Data recovery from FLASH and SSD
- PC-3000 practical classes
- Forensic analysis of incidents with examples of irretrievable data deletion Footprints of tools for irretrievable data deletion

Training 9. Mobile forensics

Duration: 8 hours

- Investigation of Android devices
- Screen lock types for Android devices. Sources of data and forensic methods for bypassing screen lock
- Investigation of iOS devices
- Data encryption in iOS
- Screen lock types for iOS devices. Sources of data and forensic methods for bypassing screen lock
- Logical and physical forensic duplication of mobile devices with UFED
- Investigation of filesystem in mobile device
- Investigation of messengers history, email history, calls history, etc.
- Data recovery from mobile devices
- Practical classes with malware application

Training 10. Practical independent investigation

Duration: 4 hours

Recommendations

Trainings 2, 3, 4 intersects in topics, but they are discussed taking into account the specifics of the operating systems.

You can create a course depending on your skills, challenges and time.

We recommend to combine trainings 2 or 3 or 4, 5, 6, 10 into one 3-day course.

The last training must be necessarily included in a course.

By agreement, each training can be prepared by us taking into account the specifics of your work.

Recommended time: from 10 a.m. till 6 p.m.

(including time for lunch)

From authors

Don't on the study of only a few trainings. Choose all of them! It can help to work more professionally. In addition, each module can be prepared at the different level of depth.

Webinar

Some trainings can be conducted as webinars.

Group-IB is one of the global leaders in preventing and investigating high-tech crimes and online fraud.

Since 2003, the company has been active in the field of computer forensics and information security, protecting the largest international companies against financial losses and reputation risks.

Group-IB's extensive experience has resulted in the innovative information security ecosystem – an array of highly sophisticated software and hardware solutions based on up-to-date threat intelligence data and deep analysis of real hacker attacks to monitor, identify and prevent cyber threats.

Official EUROPOL and INTERPOL partner

Recommended by the Organization for Security and Co-operation in Europe (OSCE)

Recognized by Gartner as a threat intelligence vendor with a strong cyber security focus

100+

successful investigations worldwide

80%

of high-profile cybercrimes in Russia and CIS are investigated by Group-IB

$70 mln

was saved by our clients due to Group-IB's products