GIAC Battlefield Forensics and Acquisition

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

GIAC Battlefield Forensics and Acquisition

Course Modules

1. Acquiring RAM and OS Artifacts

Different methods for performing acquisition of RAM, macOS and Shadow copies. This includes using disk copy utilities and target disk mode.

2. Acquisition Preparation

Summarize the goals of scene management, how to assess evidence, recognize tampering, and verify acquisitions.

3. Computer Fundamentals

Familiar with basic computer concepts, such as machine configurtn, boot processes, BIOS, UEFI, IP addressing, and domain registrars, in preparation for acquisition.

4. Data on Drives

Summarize different ways data on drives can be stored & accessed, including encryption and handling deleted files.

GIAC Battlefield Forensics and Acquisition

5. Data on the Network

Describe different ways that data can exist in motion, such as IoT network traffic and PCAP files. Discuss how different network tools can be used to discover networked devices.

6. Dead Box Acquisition

Describe the different methods for performing dead box acquisitn, including write blocking and media removal.

7. Filesystem Fundamentals

Describe basic concepts of common filesystems, like NTFS, EXT, & FAT. Describe the functionality of major components that comprise these file systems, such as Master File Tables & File Allocation Tables.

8. Host Based Live Acquisition

Describe the different methods for performing host based live acquisition, including the use of software & hardware write blocking and accessing physical drives and volumes.

9. Manual Triage

Familiar with manual techniques and tools used to select and triage data.

GIAC Battlefield Forensics and Acquisition

10. Manually Finding Data

Outline the different ways in which data can be manually found. This includes: where data can be found, carving metadata, and file recovery.

11. Mobile Device Acquisition

Describe, at a high level, the different methods used to perform mobile device acquisition. Isolating portable devices from radio signals, tools for mobile device acquisition, and identifying specific mobile devices.

12. Mobile Device Triage

Outline the ways in which data can be triaged from mobile devices. This includes Android and Apple specific scenarios and how to triage data found in mobile apps, as well as calendars and emails.

13. Physical Storage Devices

Compare and contrast the diffrnt forms of physical storage devices. This includes device interfaces, spinning disk layout, solid state drive fundamentals, and common HDD problems.

GIAC Battlefield Forensics and Acquisition

14. Remote Acquisition

Different methods for performing remote acquisitions, including acquisitions over the network as well as leveraging common cloud provider products.

15. Specialty Device Fundamentals

Describe basic concepts of common specialty devices, like MacOS, including System Profiler and Device Information Collection.

16. Storage Technologies

Summarize, compare, and contrast common storage technologies, such as the different levels of RAID configurations.

17. Using Forensic Tools for Triage

Compare and contrast the ways in which popular forensic tools can be effectively used in data triage.

18. Windows Filesystems

Compare and contrast major Windows filesystems including FAT, exFAT, and NTFS.

19. Working With Evidence Files

Compare and contrast common evidence file formats, how they can be accessed, and how they can be used in an investigation.

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474