Network Forensics

MODULE 9

Contents

Network Forensics

9.1 LEARNING OBJECTIVES

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

- Define basic concepts of networking and its role in forensics.
- Know the OSI and TCP/IP Layers and basic protocols which are pertinent for forensics.
- Define intrusion detection and prevention systems.
- Implement various techniques of capturing of network logs.

9.2 INTRODUCTION

There are many systems that track and record network activities and data. However, there are still some measures that add up to the forensics on network systems. The network forensics adds vital information to investigations. Tools can be used to do time line analysis, email re-construction, Metadata analysis, packet frame analysis or checksum on data exchanged.

Another aspect of network forensics is to make/ get capabilities of capturing and investigating a suspect's computer over network. There are methods of making an image of a suspect/ victims computer over network connection form the forensics lab itself. However, legal aspects must be considered before capturing/ intruding over other system. Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection. Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation. Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis.[3] The second form relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions. In 2000 the FBI lured computer hackers Aleksey Ivanov and Gorshkov to the United States for a fake job interview. By monitoring network traffic from the pair's computers, the FBI identified passwords allowing them to collect evidence directly from Russian-based computers.

9.3 NETWORK COMPONENTS AND THEIR FORENSICS IMPORTANCE

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices exchange data with each other along network links (data connections). The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the transmission media. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

9.3.1 Host

A network host is a computer or other device connected to a computer network. A network host may offer information resources, services, and applications to users or other nodes on the network. A network host is a network node that is assigned a network layer host address.

Computers participating in networks that use the Internet Protocol Suite may also be called IP hosts. Specifically, computers participating in the Internet are called Internet hosts, sometimes Internet nodes. Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces. The addresses are configured either manually by an administrator, automatically at start-up by means of the Dynamic Host Configuration Protocol (DHCP), or by stateless address auto-configuration methods.

Every network host is a physical network node (i.e. a network device), but not every physical network node is a host. Network devices such as modems, hubs and network switches are not assigned host addresses (except sometimes for administrative purposes), and are consequently not considered to be network hosts. Devices such as network printers and hardware routers have IP addresses, but since they are not general-purpose computers, they are sometimes not considered to be hosts.

Network hosts that participate in applications that use the client-server model of computing, are classified as server or client systems. Network hosts may also function as nodes in peer-to-peer applications, in which all nodes share and consume resources in an equipotent manner.

In operating systems, the term terminal host traditionally denotes a multi-user computer or software providing services to computer terminals, or a computer that provides services to smaller or less capable devices, such as a mainframe computer serving teletype terminals or video terminals. Other examples are a telnet host (a telnet server) and an xhost (X Window client).

9.3.2 Node

In data communication, a physical network node may either be a data communication equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment(DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

If the network in question is a LAN or WAN, every LAN or WAN nodes (that are at least data link layer devices) must have a MAC address, typically one for each network interface controller it possesses. Examples are computers, packet switches, xDSL modems (with Ethernet interface) and wireless LAN access points. Note that a hub constitutes a physical network node, but does not constitute a LAN network node, since a hubbed network logically is a bus network. Analogously, a repeater or PSTN modem (with serial interface) is a physical network node but not a LAN node in this sense.

If the network in question is the Internet or an Intranet, many physical network nodes are host computers, also known as Internet nodes, identified by an IP address, and all hosts are physical network nodes. However, some datalink layer devices such as switches, bridges and WLAN access points do not have an IP host address (except sometimes for administrative purposes), and are not considered to be Internet nodes or hosts, but as physical network nodes and LAN nodes.

If the network in question is a distributed system, the nodes are clients, servers or peers. A peer may sometimes serve as client, sometimes server. In a peer-to-peer or overlay network, nodes that actively route data for the other networked devices as well as themselves are called super nodes.

Distributed systems may sometimes use virtual nodes so that the system is not oblivious to the heterogeneity of the nodes. This issue is addressed with special algorithms, like consistent hashing, as it is the case in Amazon's.

9.3.3 Router

A router is a networking device that forwards data packets between computer networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

A router is connected to two or more data lines from different networks (as opposed to a network switch, which connects data lines from one single network). When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork.

The most familiar type of routers are home and small office routers that simply pass data, such as web pages, email, IM, and videos between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through

an ISP. More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, use of software-based routers has grown increasingly common.

9.3.4 Switch

A network switch (also called switching hub, bridging hub, officially MAC Bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device. Unlike less advanced network hubs, a network switch forwards data only to one or multiple devices that need to receive it, rather than broadcasting the same data out of each of its ports.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality that most commonly uses IP addresses to perform packet forwarding; such switches are commonly known as layer-3 switches or multilayer switches.

A switch is a device in a computer network that electrically and logically connects together other devices. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received message only to the one or more devices for which the message was intended. Each networked device connected to a switch can be identified using a MAC address, allowing the switch to regulate the flow of traffic. This maximizes the security and efficiency of the network.

9.3.5 Hub

An Ethernet hub, active hub, network hub, repeater hub, multiport repeater, or simply hub is a device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision. In addition to standard 8P8C ("RJ45") ports, some hubs may also come with a BNC or Attachment Unit Interface (AUI) connector to allow connection to legacy 10BASE2 or 10BASE5 network segments.

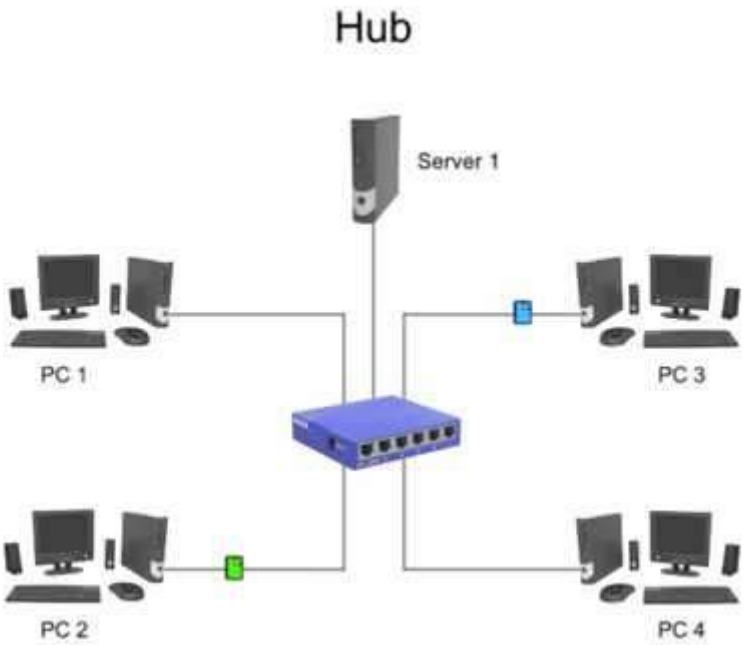
Hubs are now largely obsolete, having been replaced by network switches except in very old installations or specialized applications.

9.3.6 Network interface Card (NIC)

A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter or physical network interface, and by similar terms) is a computer hardware component that connects a computer to a computer network. A device that usually

holds the MAC (Media Access Control) address of your computer that uniquely identifies your host or computer. The NIC is the physical bridge between the network and the host. If you see on the back of your computer a wire with an oversized phone jack and blinking lights, it is NIC.

VIDEO LECTURE



This lecture is adopted from: https://www.youtube.com/watch?v=U1-2gGD9sYk
available under Creative Commons Attribution license (reuse allowed)

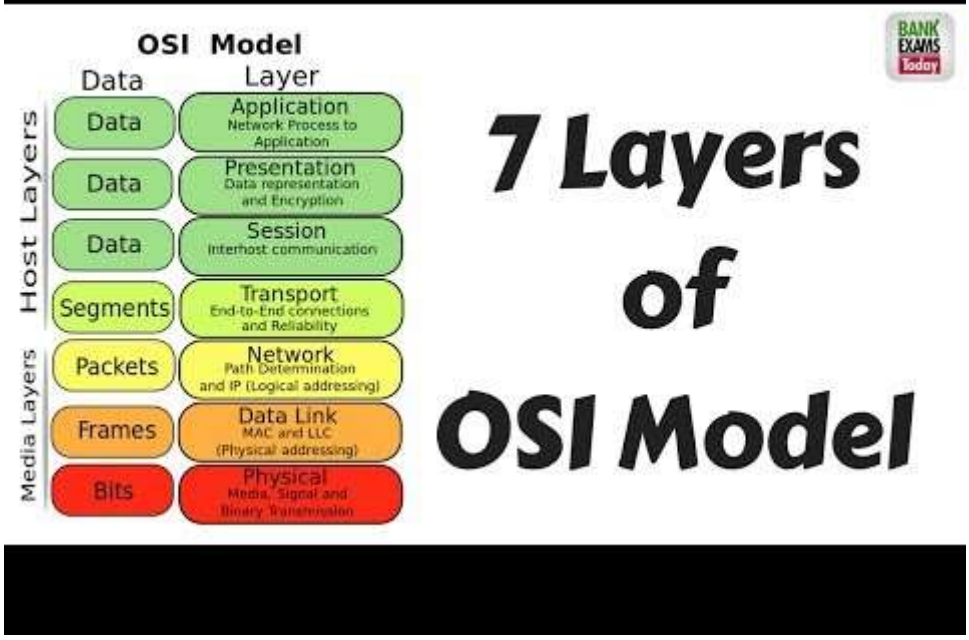
9.4 OSI

The Open Systems Interconnection model (OSI Model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.

A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that comprise the contents of that path. Two instances at the same layer are visualized as connected by a horizontal connection in that layer.

9.4.1 OSI model

VIDEO LECTURE



This lecture is adopted from https://www.youtube.com/watch?v=jY4QDTSSxBg available under Creative Commons Attribution license (reuse allowed)

The OSI (Open System Interconnection) is a standard logical view of any networking. It has 7 layers as given in *Figure 1*. *Figure 1* also depicts various form of data formats that are exchanged between each layers of either side in a connectivity. It also gives main functionalities of each layer as abstracted.

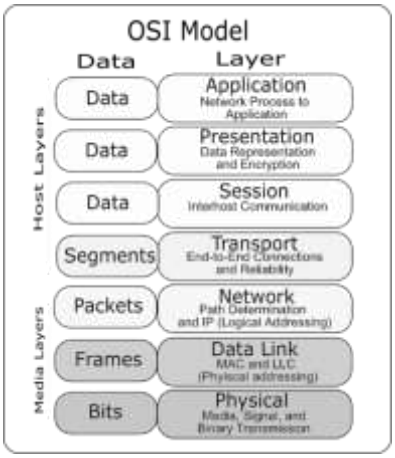


Figure 1: OSI Layers

9.4.2 TCP/IP Layers

Although the OSI model is widely used and often cited as the standard, TCP/IP protocol has been used by most UNIX workstation vendors. TCP/IP is designed around a simple four-layer scheme. It does omit some features found under the OSI model. Also it combines the features of some adjacent OSI layers and splits other layers apart. The four network layers defined by TCP/IP model are as follows (also given in the figure 2):

- Layer 1 – Link: This layer defines the network hardware and device drivers.
- Layer 2 – Network: This layer is used for basic communication, addressing and routing. TCP/IP uses IP and ICMP protocols at the network layer.
- Layer 3 – Transport: Handles communication among programs on a network. TCP and UDP fall within this layer.
- Layer 4 – Application: End-user applications reside at this layer. Commonly used applications include NFS, DNS, arp, rlogin, talk, ftp, ntp and traceroute.

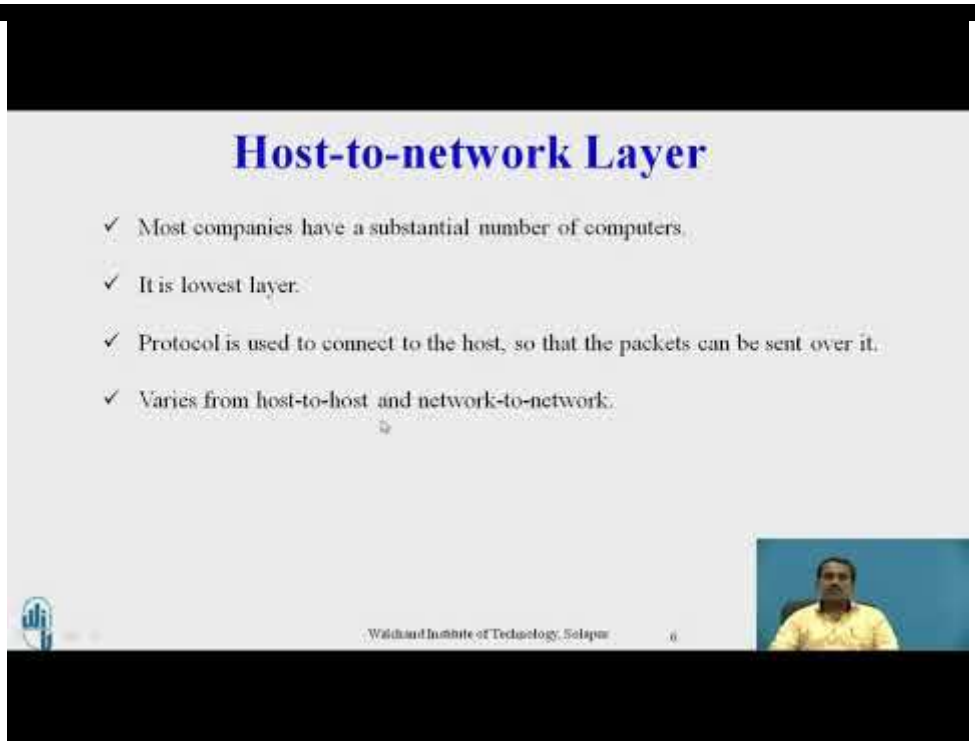
The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks. It is commonly known as TCP/IP, from Transmission Control Protocol (TCP) and the Internet Protocol (IP). TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination. This functionality is organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved. From lowest to highest, the layers are the link layer, containing communication technologies for a single network segment (link); the internet layer, connecting hosts across independent networks, thus establishing internetworking; the transport layer handling host-to-host communication; and the application layer, which provides process-to-process application data exchange.

The TCP/IP model and related protocol models are maintained by the Internet Engineering Task Force (IETF).

Encapsulation is used to provide abstraction of protocols and services. Encapsulation is usually aligned with the division of the protocol suite into layers of general functionality. In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers, being further encapsulated at each level.

The layers of the protocol suite near the top are logically closer to the user application, while those near the bottom are logically closer to the physical transmission of the data. Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols from the details of transmitting bits over, for example, Ethernet and collision detection, while the lower layers avoid having to know the details of each and every application and its protocol.

VIDEO LECTURE



This lecture is adopted from https://youtu.be/x_aZbwQPFuc available under Creative Commons Attribution license (reuse allowed)

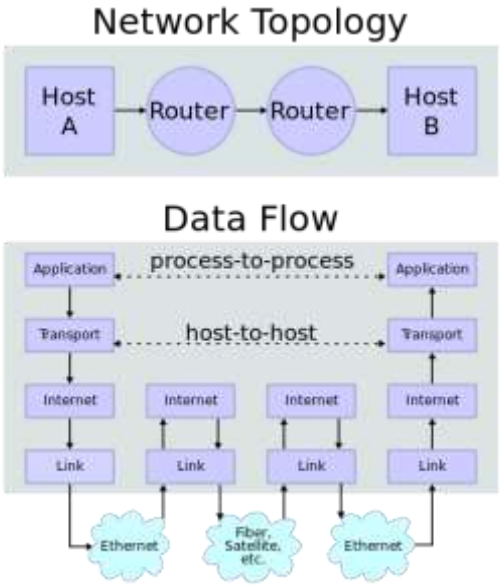


Figure 2:Internetworking.

Figure 2 depicts two Internet hosts connected via two routers and the corresponding layers used at each hop. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe. Every other detail of the communication is hidden from each process. The underlying mechanisms that transmit data between the host computers are located in the lower protocol layers.

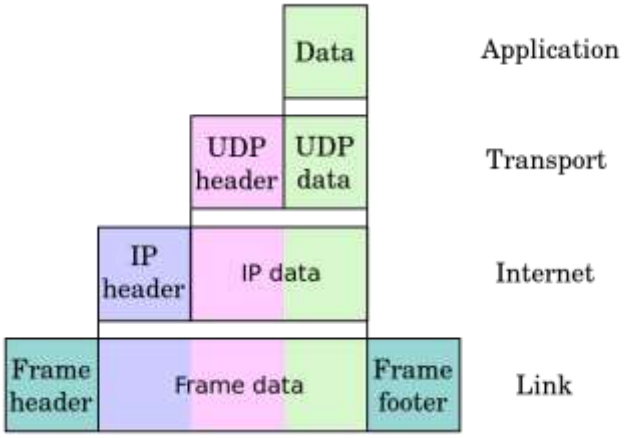


Figure 3: Encapsulation of application data descending through the layers

Applying forensic methods on the Ethernet layer is done by eavesdropping bit streams with tools called monitoring tools or sniffers. The most common tool on this layer is Wireshark (formerly known as Ethereal) and tcpdump where tcpdump works mostly on unix-like operating systems. These tools collect all data on this layer and allow the user to filter for different events. With these tools, websites, email attachments, and other network traffic can be reconstructed only if they are transmitted or received unencrypted. An advantage of collecting this data is that it is directly connected to a host. If, for example the IP address or the MAC address of a host at a certain time is known, all data sent to or from this IP or MAC address can be filtered.

To establish the connection between IP and MAC address, it is useful to take a closer look at auxiliary network protocols. The Address Resolution Protocol (ARP) tables list the MAC addresses with the corresponding IP addresses.

To collect data on this layer, the network interface card (NIC) of a host can be put into "promiscuous mode". In so doing, all traffic will be passed to the CPU, not only the traffic meant for the host.

However, if an intruder or attacker is aware that his connection might be eavesdropped, he might use encryption to secure his connection. It is almost impossible to break nowadays encryption but the fact that a suspect's connection to another host is all the time encrypted might indicate that the other host is an accomplice of the suspect.

On the network layer the Internet Protocol (IP) is responsible for directing the packets generated by TCP through the network (e.g., the Internet) by adding source and destination

information which can be interpreted by routers all over the network. Cellular digital packet networks, like GPRS, use similar protocols like IP, so the methods described for IP work with them as well.

For the correct routing, every intermediate router must have a routing table to know where to send the packet next. These routing tables are one of the best sources of information if investigating a digital crime and trying to track down an attacker. To do this, it is necessary to follow the packets of the attacker, reverse the sending route and find the computer the packet came from (i.e., the attacker).

The internet can be a rich source of digital evidence including web browsing, email, newsgroup, synchronous chat and peer-to-peer traffic. For example web server logs can be used to show when (or if) suspect accessed information related to criminal activity. Email accounts can often contain useful evidence; but email headers are easily faked and, so, network forensics may be used to prove the exact origin of incriminating material. Network forensics can also be used in order to find out who is using a particular computer by extracting user account information from the network traffic.

9.5 SUMMARY

1. Network forensics is a sub-branch of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection.
2. Network components like host, node, router, switch, hub, NIC etc. all have to be considered while examining a network forensically.
3. OSI and TCP/IP layers needs to be understood while doing forensics over networks.
4. Applying forensic methods on the Ethernet layer is done by eavesdropping bit streams with tools called monitoring tools or sniffers like wireshark and tcpdump.
5. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. The logs generated by the IDS can be very useful for network forensics analysis.

9.6 CHECK YOUR PROGRESS

1. Fill in the blanks.

i. Computers participating in networks that use the Internet Protocol Suite may also be called _____.
ii. Modem, hub, bridge or switches are _____ in a data communication.
iii. Digital telephone handset, a printer or a host computer are called as _____ in a data communication.
iv. A _____ is a networking device that forwards data packets between computer networks. Routers perform the _____ functions on the Internet.
v. A _____ is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

vi. A _____ is a computer hardware component that connects a computer to a computer network.

vii. TCP/IP model has basically 4 layers they are: _____, _____, _____, _____ Layers.

2. State True or False

i. Generally forensics makes use of agents (Software) to gather and send Host data to remote forensic server.

ii. Routers have a CAM (context addressable memory) which keeps information about mappings of MAC address to ports.

iii. Firewalls are example of IDS.

9.7 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) IP hosts.
b) data communication equipment (DCE).
c) data terminal equipment(DTE.
d) router , "traffic directing".
e) network switch .
f) A network interface controller .
g) Link, Network,Transport, Application.

2. State True or False

i. (T)
ii. (F)
iii. (F)

9.8 FURTHER READINGS

1. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
2. Investigating Hard Disks, File and Operating Systems: EC-Council | Press
3. Gary Palmer, A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, August 7 – 8, 2001, Page(s) 27–30

9.9 MODEL QUESTIONS

1. State and explain various network components and their forensic importance.
2. How are the network logs captured and analysed? Explain.
3. What are IDS and IDPS?

References, Article Source & Contributors

[1] Computer network - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Computer_network

[2] Ethernet hub - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Ethernet_hub

[3] Forensic data analysis - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Forensic_data_analysis

[4] Host (network) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Host_(network

[5] Intrusion detection system - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Intrusion_detection_system

[6] Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.

[7] Network forensics - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_forensics

[8] Network interface controller - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_interface_controller

[9] Network switch - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_switch

[10] Network tap - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_tap

[11] Network Time Protocol - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_Time_Protocol

[12] Node (networking) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Node_(networking)

[13] OSI model - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/OSI_model

[14] Port mirroring - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Port_mirroring

[15] Promiscuous mode - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Promiscuous_mode

[16] Router (computing) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Router_(computing)

[17] TCP/IP 4 layer model, http://www.planetlarg.net/tcpip-4-layer-model

[18] tcpdump - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Tcpdump

[19] Wireshark - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Wireshark

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