Book 6 - Network Forensics

1. Introduction to Network Forensics

Scope Template	
Number	1
Title	Introduction to Network Forensics
Introduction	This chapter introduces and defines Network Forensics, which is a field of digital forensics. It starts with an exploration of general security concepts such as: information security, network security, host security, traffic analysis, network devices, digital evidence, logging, etc. It presents the case for network forensics, including why and how it differs from digital forensics. It describes network evidence and how it can be used in forensic investigations; the types, the sources of such evidence and the challenges we might face during its collection . We subsequently discuss network forensics data types and the differences between these types. Finally , we introduce a methodology to follow during network forensic investigations called OSCAR, which consists of steps to be executed in sequence. These steps are: Obtain information, strategize, collect evidence, analyze and finally report.
Outcomes	On successful completion of this chapter, the student should be able to • This chapter summarize some basic concepts about digital forensics in general and network forensics in specific. • Describe the forensic evidence retrievable from network devices • Describe the process of forensic data collection and related challenges • Apply a suitable methodology while investigating an incident. The student will be introduced to the OSACR methodology, which is a good example of such a methodology.
Topics	1. Introduction 2. Host and Network device security 3. Network Forensics 3.1 Network Forensics vs. Digital Forensics 3.2 Why Network Forensics 4 Network-based evidence 4.1 Network-based Evidence Sources 4.2 Challenges Relating to Network Evidence 5 Network Forensic Data 5.1 Network Forensic Data Types 5.2 Network Forensic Data Type Comparison 6 Network Forensics Investigative Methodology (OSCAR) a) Obtain Information b) Strategize c) Collect Evidence d) Analyze e) Report 7 Summary
Study Guide	• Required study time. ○ 12 hours • Required hardware/software. ○ None • Required external resources including links and books. ○ Network Forensics : Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012, ISBN:0-13-256471-8 ○ NIST Publication 800-86 (https://csrc.nist.gov/publications/detail/sp/800-86/final)

	○ ISO 27000 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en)

Content Template	
Section Number	1.1
Section Title	Introduction
Introduction	In this section, we start our discussion of network forensics. Network forensics is a field of "Digital Forensics**"**, which is sometimes also called "File Forensics". In this book, we apply the science of digital forensics to networked environments. The fundamental concepts remain the same, but the techniques differ because of the nature of the forensics data and the devices that data resides on. This chapter presents the main concepts that are related Network forensics.
Content	The concept of Network Forensics is of increasing importance because of the growing usage of networks and their applications. In many cases and for various reasons, an investigator or network defender will not find persistent forensic data residing on devices where data has been transmitted through the air or over wires. It is a challenge to detect, collect and subsequently analyze this traffic in order to reach conclusions on a breach or collect reliable and admissible digital evidence. In the next section, we briefly discuss the security and forensics of networked hosts and devices, which are the theatres of any forensic investigation. In section 3, we define network forensics and differentiate between network forensics and digital forensics. In section 4, we explore the sources of network-based evidence. In section 5, we examine the various Forensic Data Types. In section 6, we introduce the Network Forensics Investigative Methodology (OSCAR) and we conclude this topic with a summary in section 7.

Content Template	
Section Number	1.2.1
Section Title	Host security
Introduction	The host can be a server or client machine in the network. The main goal of network security is to protect the confidentiality, availability and integrity of hosts and their data. In this section, we define hosts, explain the importance of host security, and introduce some concepts related to hosts and network forensics.
Content	Host are devices (laptops, smartphones, workstations, etc.) on the network must always be protected and in case of a penetration or an attack should be analyzed correctly to calculate damage and implement appropriate incident response. In order to support such an analysis and to provide continuous monitoring capabilities, each host should be capable of storing logs or historical data recording events and network traffic of potential interest to the forensic investigator. Hosts may be high-end computers such as local servers or cloud servers. They can be client computers such as desktops, laptops, tablets, smartphones, cloud hosts, virtual hosts, Web hosts, etc. Hosts may also be virtual machines that are used as both servers and clients. Hosts are often the target of an attack or attempted penetration because they contain: 1. Potentially sensitive data. 2. environments that, if compromised, can be used to attack targets and hide tracks. 3. Information systems and programs (binaries and source code). 4. Access databases, authentication processes and techniques and authorization data. 5. Network services such as e-mail, web, chat applications and application servers. Network forensics is a branch of digital forensics that includes host based forensics which is usually crucial to any investigation process. its importance stems from two observations: 1. Host are usually the target of a network attack. Even though an attacker might be interested in attacking a router to disrupt service, he more dangerous attack is the one that involves data theft or vandalism. 2. Hosts are a rich source of forensics data.

Content Template	
Section Number	1.2.2
Section Title	Network device security
Introduction	Active network components such as routers, switches, firewalls, access points, sensors, Wireless access points (WAPs) , etc. are very important to network security and forensics. In this section, we explore these devices and consider some of the threats that might affect them.
Content	Network devices 1. Routers (Network **layer)** Routers are a core component of any network. A router connects the local network to other networks and the internet. Because of this, routers are sometimes the target of an attack or are used to gain access to a network. Thus, it is very important to protect routers in the first instance. In case of an attack or penetration, routers should be able to provide any information that can help in investigating the event . Routers contain routing tables rules and configuration parameters such as bandwidth, QoS, delay, distance, load and other important information. 2. Switches (data link and network layer) Switches connect the devices in the network together. They are usually not a target of an attack, but would be used to do so and might contain some information that might help with the analysis. 3. Firewalls (network and transport layer) Firewalls are network devices that are used to protect networks by controlling the ingress and egress of traffic. It would be disastrous from a security viewpoint if they were disabled or compromised 4. Access points (data link layer) Access points are devices that are used to enable wireless access to networks. They are usually connected to the traditional network infrastructure. With a growing trend of BYOD, such wireless access points are becoming more critical. 5. Wireless modems and routers Devices used to connect home and office networks to ISP networks through ADSL or Fiber. 6. IoT Sensors (application layer and network layer) An IoT sensor is a light weight device that may transmit important data. The data transmitted by and residing on on such sensors could be industrial data, health data, city and home security data and so on. As mentioned earlier, network devices might not be the target of an attack, but can be the stepping stone used. They have important data that can be used for analysis and investigation.

Content Template	
Section Number	1.3
Section Title	Network Forensics
Introduction	In this section, we introduce and define network forensics, which is a field of digital forensics. We will briefly discuss the difference between network forensics and digital forensics. We briefly discuss requirements, procedures and implications of network forensics.
Content	Digital Forensics Definition(s): CNSSI 4009-2015 (DoDD 5505.13E) defines digital forensics as an approach to digital investigation that applies the fundamentals of computer science and mathematics to provide procedures and tools for examining, validating, searching and reporting the existence of digital evidence. NIST SP 800-86 also defines digital forensics as an application of computer science whose aim is to identify, collect, examine, and analyze data, where the integrity of the information is preserved. Source(s): NIST SP 800-86 Palmer [1] defines Network Forensics as a branch of digital forensics whose aim is to monitor and analyze the information gathered from network traffic to provide intrusion detection and legal evidence. [1] 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

Content Template	
Section Number	1.3.1
Section Title	Digital Forensics vs. Network Forensics
Introduction	As mentioned earlier, network forensics is part of the broader discipline of digital forensics. However, with the massive growth of networking (wired and wireless) and with cloud computing and virtualization becoming ubiquitous, network forensics can be considered a separate but closely related discipline.
Content	Following are some differences between digital and network forensics: • Digital Forensics: 1. Data is static and preserved even if power is cut. 2. Evidence is contained within the file system. 3. Making a forensically sound image is straightforward. 4. Seizing a computer to obtain evidence might involve disruption to the existing file, storage and logs. 5. Legal precedence in place and derived evidence is routinely admitted into court. • Network Forensics: 1. Data is changing constantly (dynamic). 2. Pinpointing exact location of required evidence is problematic since this may involve direct evidence that can be obtained directly from single network device and some evidences can indirectly obtained from several network devices. 3. Physical access to network devices can be difficult to obtain due to some geographical and legal constraints. 4. Most network devices do not have persistent data storage. 5. Investigators must minimize investigation impact on live business networks. 6. Conflicting precedence and lack of standardization means courtroom admissibility is not guaranteed. 7. Network Forensics requires deep understanding of network protocols and routing protocols such as Border Gateway Protocol (BGP), Interior Gateway Routing Protocol (IGRP) Routing Information Protocol (RIP), Ethernet, ARP, IP, TCP/UDP and a myriad of application layer protocols. Reference: Davidoff, Sherri, and Jonathan Ham. Network forensics: tracking hackers through cyberspace. Prentice hall, 2012.

Content Template	
Section Number	1.3.2
Section Title	Why Network Forensics?
Introduction	Network forensics is of growing importance for many reasons. as mentioned earlier, we are now living in a more interconnected world, which requires analysis and investigation of inappropriate or illegal network usage. Here, we explore the importance the field by answering the question "Why Network Forensics?".
Content	Why worry about Network Crime / Forensics? 1. The malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016".. 2. Attacks can come from both inside and outside of the network. 3. Attackers are no longer basement hackers: a) Employees Disgruntled employees might seek to damage employers for many reasons. b) Business competition some competing businesses try to hack into each other's systems to steel information or cause damage. c) Professional hackers for hire It is easy now to find professional hacking services on the dark web . d) State actors Many states are now conducting campaigns against entities and infrastructure in other states for political or economic reasons. Examples: 1. Russia political Hacking; Russian Hacking and Influence in the U.S. Election [1], Twelve Russians charged with US 2016 election hack [2] 2. China's economic hacking on the US [3] 3. Stuxnet [1] https://www.nytimes.com/news-event/russian-election-hacking [2] https://www.bbc.com/news/world-us-canada-44825345 [3] https://www.wired.com/story/china-hacks-against-united-states/
Content Template	
Section Number	1.4
Section Title	Network-based Evidence
Introduction	In this section, we introduce Network-based evidence and its sources.
Content	Electronic Evidence Definition(s):

	Information and data of investigative value that is stored on or transmitted by an electronic device. This includes text files, audio, videos and digital images. Source(s): NIST SP 800-72 Digital Evidence Definition(s): Information in electronic binary form stored or transmitted over the network. in binary form. Source(s): NIST SP 800-101 Rev. 1 NIST SP 800-72

Content Template	
Section Number	1.4.1
Section Title	Network-based Evidence Sources
Introduction	Network environments are usually varied, but they all rely on network devices such as: routers, firewalls, switches, etc. (See section 1.2.2.) Generally, there are multiple sources of evidence in a network that can be used for forensics.
Content	Network-based evidence sources: 1. Packets transmitted over wired and wireless links 2. Switches 3. Routers 4. DHCP Servers 5. Name Servers 6. Authentication Servers 7. Network IDS/IPS 8. Firewalls 9. Web Proxies 10. Application Servers 11. Central Log Servers

Content Template	
Section Number	1.4.2
Section Title	Challenges Relating to Network Evidence Collection and Analysis
Introduction	There are challenges when working with evidence that needs to be collected and analyzed in a networked environment. Some of these challenges are similar to those faced when working with host/file-system/static forensics.
Content	challenges include : 1. Acquisition: It is difficult to locate and access specific evidence in a network due to many reasons, for example, evidence could reside in different locations such as in network logs, on proxies and access points. Moreover, the transformation of evidence from a machine-readable to a more meaningful format brings further challenges . . 2. Content: 3. The granularity of data residing on Network devices is often different to that found in traditional file systems. For example, due to the storage limitations of some network devices only specific metadata about the transactions and transfer of data are recorded Storage: 4. Data may be volatile because many devices in the network do not contain persistent or even secondary storage, and, as a result, much digital evidence could be corrupted, lost and/or damaged.Privacy: 5. Privacy and legalization could improve several concerns in term of accessing personal data over network. However some privacy and legalization could impose difficulties to the investigators for accessing and obtaining access for the network devices and storage data. Environment. Seizure: Finding specific digital evidence in some cases requires manipulation of large network segments. Especially the networks that are distributed among different geographical areas and which may require to comply with multiple legalization and authoritative rules. 6. Admissibility: The conventional evidence that is extracted from file systems is now becoming widely acceptable in both civil and criminal legal proceedings . However, evidence extracted from network devices may not be so readily admitted in court. . H. Marshall Jarrett, Director, EOUSA, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," 204.
Content Template	
Section Number	1.5.1
Section Title	Network Forensic Data
Introduction	Network-based forensic data is data residing on network devices or passing through a transmission medium (either wired or wireless).
Content	Network forensic data is typically grouped into three main data types based on the associated tools and analysis techniques used: 1. Full packet capture (PCAP)

	• A full copy of packets travelling over the network is captured. • Supports The most complete form of monitoring possible. • Requires considerable storage capacity. . Packet Brokering may be used to come up with scalable architecture for the data. 2. Flow data (netflow) • Records summary data of conversations on the network. • Stores information such as time, duration, number of packets, total bytes sent, received, etc. • No application layer data recorded. • Suitable for gaining a quick understanding of how data flows on the network . 3. Log / alert data (giant text files) • text records are written to a file and the file is monitored . • Records of varying importance with high priority alerts generated by firewalls, IDs, IPs, etc. • • There are a lot of log sources, so a management interface is required. Tools (e.g. Splunk) to explore large files of text records will also aid the investigative process and the data management task. .

Content Template	
Section Number	1.5.2
Section Title	Network Forensic Data Type Comparison
Introduction	In this section, a comparison of the three types of network forensics data is presented.
Content	

	Collection	Storage	What it can reveal	Tools used to Analyze	Typical use
PCAP	Done by machines on the network, taps, and anything that can read 1's and 0's off the network	Consumes lots of disk space. For a project of any size, you'll have to spend money on a storage solution.	**Exactly** what went across the network.	Wireshark, Firewalls, Content Filters, etc.	Deep dive, finding out exactly what commands were issued and how compromises occurred.
Flow	Done by apps on computers on the network or by decent routers	Low space requirements, so it's easy. Generally unified for large networks.	Patterns about conversations, amount of data sent, time, etc.	Silk, Argus, etc.	Retrospective analysis, finding attackers and compromised machines.
Log/Alert	Done by whatever app creates them, wherever it's set to write them.	Generally either left where they were created or consolidated by a log manager or SIEM	Events that occur and are noticed by some piece of software, e.g. attacks, outages, etc.	Splunk, Arcsight, SIEM's	Alerting us to major problems when they occur (or as soon as our log handling methodology shows it to us)

Fig. 1

1 Jim Irving

Content Template	
Section Number	1.6
Section Title	Network Forensics Investigative Methodology (OSCAR)
Introduction	In this book, we adopt the methodology proposed by Davidoff and Ham [Ref] to network forensics. In this section, we introduce this methodology and the processes that underpin it.
Content	The methodology consists of five phases or stages that are followed in sequence while managing the life-cycle of the network forensic investigation. The methodology is usually referred to as the OSCAR methodology and consists of the following phases: a. Obtain Information b. Strategize c. Collect Evidence d. Analyze e. Report In the following sections, we briefly discuss each stage. Ref : Davidoff, Sherri, and Jonathan Ham. Network forensics: tracking hackers through cyberspace. Prentice hall, 2012.

Content Template	
Section Number	1.6.1
Section Title	OSCAR Obtain Information
Introduction	In this section, we introduce the first step in the Forensics process i.e. "Obtain Information". By "Obtain Information", we mean the collection of any information that is related to system environment and incident under investigation. .
Content	a) The incident an investigator typically begins by gathering the following incident-related information: • Description of the case • The time and the date of the case • Identification of the people involved • Identification of the data and the system components involved • Identification of any process or actions performed since incident discovery • Identification of processes for managing the incident • Identification of any legal concerns • deadlines for the investigation and recovery for the data b) The environment The investigator should study the technical and organizational environment in which the incident took place. The investigator should try to assess the following: • The deployed business model • Legal concerns • The topology of the network • Identification of network evidence resources • The organizational infrastructure and communications systems • The process and procedures for the incident response • The availability of resources in term of budget, time and equipment •

Content Template	
Section Number	1.6.2
Section Title	OSCAR Strategize
Introduction	In this section, we introduce the second step in the Forensics process, i.e. "Strategize".
Content	An investigator should have a strategy for dealing with an incident. For example, time management is very important especially when dealing with volatile data in networks. Also, a suitable plan to deal with the various evidence sources is required. a high degree of coordination with other investigating team members and the customer / victim is required. The authors in our reference [ref] recommend the following steps when developing an investigation strategy: • Identification of time-frame for completion and the objectives of the investigation. • Identification of resources in term of budget, time and equipment. • Identify any possible evidence sources. • Estimation of the evidence acquisition cost. • Prioritization the evidence. • Plan the evidence acquisition and analysis processes. • • The acquisition is an iterative process that may require several iterations before all necessary data is acquired. This may necessitate additional time, cost and more equipment.

Content Template	
Section Number	1.6.3
Section Title	OSCAR Collect Evidence
Introduction	In this section, we introduce the third step in the Forensics process, i.e. "Collect Evidence".
Content	evidence collection is the third step in the OSCAR methodology . There are three components to the collection phase : • Document All evidence should be carefully documented in logs that record all the steps performed during the evidence collection process. The investigation steps followed and the accompanying notes could be useful references for courts and during the analysis phase. The documentation also serves as an important audit trail for the investigation process. • Capture • The evidence capturing process may involve analysis of different network resources such as system and server logs, system proxies and many other resources. All evidence should be preserved on suitable media. Store and transport A Chain of custody process should be implemented to store a evidence safely in a verifiable log that that can be securely signed by all the investigation process stakeholders. The evidence collection process has major implications when it comes to assessing the admissibility in court of any evidence presented. Thus a well-defined and strictly adhered to process is required from the collection, storage, transfer phases through to return to owner. Several best practices are involved during the investigation process such as creating verifiable evidence copies that are managed using cryptographic tools and keeping the original files protected using a strict custody management process. The investigation should be run on the verifiable copies and the originals should remain untouched.

Content Template	
Section Number	1.6.4
Section Title	OSCAR Analyze
Introduction	In this section, we introduce the fourth step in the Forensics process, i.e. "Analyze".
Content	The analysis step follows evidence collection. in most cases, in its raw form, collected evidence will be massive, fragmented and meaningless . During the analysis step, multiples concepts are applied such as: • Correlation: One of the first issues in analysis is how to correlate data collected from different sources and of different types. The correlation process can be either manual or automatic using state of the art computer science technologies such as Artificial Intelligence (AI). • investigation Timeline: • Identification of data sources is required at this stage and a timeline of activities is developed to specify the time and the method used during the process of investigation. Events of Interest: Identification and isolation of the most important. • Corroboration: In some cases the collection of data from multiple sources of network and system logs may produce false positives . As a result, evidence should be corroborated across multiple sources to enhance trust levels. • Interpretation: Understanding and Interpretation of findings are essential during the investigation process. Investigators may have their own hypotheses that need to be proved before presentation to a court. .

Content Template	
Section Number	1.6.5
Section Title	OSCAR Report
Introduction	In this section, we introduce the fifth step in the Forensics process, i.e. "Report".
Content	It is very important for an investigator to be able to amalgamate all results and steps into a professional and convincing report . Most forensics tools are able to generate reports that can be customized to suit specific needs. However, the investigator should be able to write reports professionally in response to any request by a court or authorized business. The produced report must be: • clear and meaningful for non-technical people, such as: – Legal stakeholders, e.g. Juries and Judges – Project Managers – Human Resources personnel • defendable and accurate In general, the report should be easy to understand, while maintaining professionalism.

Content Template	
Section Number	1.7
Section Title	Summary
Introduction	In this section, we present a quick review of the previous sections and conclude our first chapter.
Content	In this first chapter of our Network Forensics Book, we have introduced fundamental concepts in digital forensics and network forensics. In section 1, we introduced the subject. In section 2, we discussed host security and network device security and types, which are often the target or medium of any incident or attack. In section 3, we introduced definitions of network forensics and digital forensics and we explained that network forensics is a sub process of digital forensics with some highlighted differences. We also discussed why network forensics should be treated as a separate discipline. In section 4, we presented network-based evidence; its importance, types and sources. We outlined the challenges we might face when collecting evidence from these sources. In section 5, we described network-based evidence data types such as packet captures, net flows and logs. We explored in some detail the differences between these types in terms of their collection, storage, value, tools, etc. In section 6, we introduced the OSCAR method for network forensics investigation, which is a method we adopted from Davidoff and Ham. The methodology has five steps, which are: Obtain data, Strategize, Collect evidence, Analyze, and report. In the following chapters, we delve more into the details of Network Forensics.

Activity Template	
Number	1.2.2
Title	Network device security
Type	Review
Aim	The student will learn to Explore Some basic concepts regarding digital forensics in general and network forensics in specific.
Description	Login (asking a network administrator for help if required) to the router providing internet connectivity to your computer. Construct a table listing core router network configuration parameters like DNS servers, IP addresses, etc. . For each configuration parameter comment on how this data might be used in a forensic investigation.
Timeline	1 Hour
Assessment	The instructor grades the reports and returns them to students.

Activity Template	
Number	1.3.2
Title	Why Network Forensics
Type	Reflection
Aim	• To understand the impact of political or economic hack and the role of forensics.
Description	Go to one of the following web sites and write a one-page report on a political or economic hack and the role of forensics in that case. [1] https://www.nytimes.com/news-event/russian-election-hacking [2] https://www.bbc.com/news/world-us-canada-44825345 [3] https://www.wired.com/story/china-hacks-against-united-states/
Timeline	1.5 hours to read the article 1.5 hours to write the report Total 3 Hours
Assessment	The instructor grades the reports and returns them to students.

Activity Template	
Number	1.4.1
Title	Network-based Evidence Sources
Type	Research
Aim	• Acquire the required basic knowledge regarding network devices that contain forensic data.
Description	Go to Section 1.4.1 and write a 2-3 lines for each source listed in the section outlining your expectations of how this source would be used in a forensic investigation.
Timeline	2 hours
Assessment	The instructor grades the reports and returns them to students.

Activity Template	
Number	1.5.1
Title	Network Forensic Data
Type	Research
Aim	• Examine the process of the forensic data acquisition and analysis .
Description	For each of the three types of forensic data defined in section SCAIT-C1-section 1.5.1 list the top five tools for handling it, whether commercial or open-source.
Timeline	3 Hours
Assessment	The instructor asks the students to briefly talk for 1-2 minutes about one of the tools he/she has researched.

Activity Template	
Number	1.6
Title	Network Forensics Investigative Methodology (OSCAR)
Type	Review Research
Aim	ntroduce students to the OSACR methodology, which is a very good example of a network forensics investigative methodology.
Description	Go to section 1.6 and review the listed forensics methodology steps. 1. Write a short paragraph describing each step 2. Conduct online research looking for tools that can be used in each step.
Timeline	1 hour for write-up 2 hours for tool research Total 3 Hours
Assessment	Report to be graded and the instructor to ask the students to briefly discuss for 1-2 minutes one of the tools identified and the step in the methodology that it covers.

Think Template (MCQs)	
Number	1.2.2
Title	Network device security
Type	Multiple Choice Question: Choose the correct answer
Question	Which of the following is a network device that might be part of an forensic investigation: a) Router b) Switch c) Firewall d) All of the above
Answers	All of the above.

Think Template (MCQs)	
Number	1.3
Title	Network Forensics
Type	Fill in the blank
Question	Network forensics is ---------- of digital forensics relating to the monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence, or intrusion detection
Answers	A sub-branch

Think Template (MCQs)	
Number	1.4.1
Title	Network-based Evidence Sources
Type	Multiple Choice Question: Choose the correct answer
Question	Which of the following is not a source of network-based evidence: a) DHCP Servers b) Authentication Servers c) Network IDS/IPS d) Application Servers e) Fiber Cables
Answers	e) Fiber Cables

Think Template (MCQs)	
Number	1.5.1
Title	Network Forensic Data
Type	Multiple Choice Question: Choose the correct answer
Question	Which of the following choices belong to one of the network forensics data types a) Records of conversations on the network b) Stores info such as time, duration, number of packets, total bytes sent, received, etc. c) any information stored in the application layer data d) understanding how data flows on your network quickly
Answers	b) Stores info such as time, duration, number of packets, total bytes sent, received, etc.

Think Template (MCQs)	
Number	1.6
Title	Network Forensics Investigative Methodology (OSCAR)
Type	Multiple Choice Question:
Question	The OSCAR methodology consists of five phases or stages that are followed in sequence while managing the life cycle of a network forensics investigation . Which of the following is not a stage in the OSCAR methodology: a) Obtain Information b) Information optimization c) Collect Evidence d) Analyze e) Report
Answers	b) Information optimization f.

Think Template (MCQs)	
Number	1.4
Title	Network-based Evidence
Type	Fill in the blank
Question	Electronic Evidence is information and data of investigative value that is stored on or transmitted by an electronic device. Provide three samples of these information and data ----------.
Answers	Text files, audio, videos and digital images.

Think Template (MCQs)	
Number	1.2.1
Title	Host security
Type	Fill in the blank
Question	Hosts can be high-end computers such as local servers or cloud servers. They can be client computers such as ----------.
Answers	Desktops, laptops, tablets, smart phones, cloud host, virtual host, web host. etc.

Extra Template	
Number	1.1
Title	Network Forensics Book (Introduction)
Topic	Link to the corresponding section and topic. 1.6 Network forensics Methodology (OSCAR)
Type	Book/Chapter (ISBN) Network Forensics : Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012, ISBN:0-13-256471-8

Extra Template	
Number	1.2
Title	Open Security Training,
Topic	1.4 Security-Related Reversing 1.5 Reversing Cryptographic Algorithms
Type	Eldad Eilam, Reversing: Secrets of Reverse Engineering John Wiley & Sons, Inc. New York, NY, USA ©2005 ISBN: 9780764574818

Extra Template	
Number	1.3
Title	Network Forensics
Topic	2.1 File extensions and File signatures
Type	John Sammons, The Basics of Digital Forensics, Second Edition: The Primer for Getting Started in Digital Forensics 2nd, Syngress Publishing ©2014 ISBN:0128016353 9780128016350

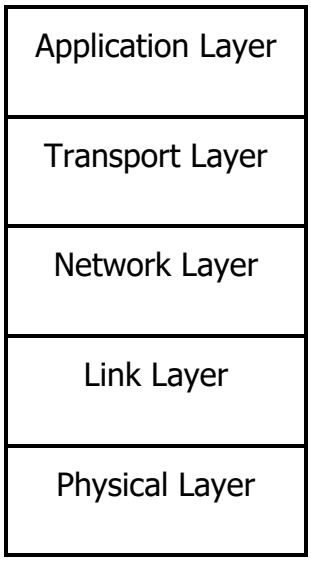
Extra Template	
Number	1.4
Title	Network-based Evidence
Topic	2.4 Policies
Type	URL: https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

2. Network Foundations and Protocols

Scope Template	
Number	2
Title	Network Foundations and Protocols
Introduction	This chapter reviews network service models and some of the important protocols, in addition to network tunneling in the context of network forensics. It discusses key protocols including IPv4, IPv6, IPsec, TCP, and UDP. This chapter is intended to provide a technical and conceptual foundation for upcoming chapters.
Outcomes	After completing this chapter, the student will gain the following: • The ability to differentiate between network service models and the importance of layering concept. • The ability to understand, analyze and interpret TCP/IP protocols. • The ability to explain network tunneling in the context of network forensics and its implications for the network forensics investigator
Topics	2. Network Foundations and Protocols 2.1. Network Protocol Stack 2.2. Internet Protocol 2.3. Internet Protocol Security 2.4. User Datagram Protocol 2.5. Transmission Control Protocol 2.6. Network Tunneling
Study Guide	• Required study time. ○ 21 hours • Required hardware/software. ○ None • Required external resources including links and books. ○ Network Forensics: Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012, ISBN: 0-13-256471-8.

Content Template	
Section Number	2.1
Section Title	Introduction
Introduction	In this section, we provide an introduction to networking and we discuss the importance of understanding networking principles and protocols for the network forensics investigator.
Content	The current Internet consists of billions of connected devices all over the globe. The Internet service model governs the communication between these devices through the use of various protocols operating at different layers in the network service model. The role of protocols is to facilitate the communication between communicating devices. Protocols govern the way messages are transmitted and received. Also, protocols define the message format and the meaning of its content. However, attackers try to by-pass these protocols in order to hide data or to conduct various types of attacks. Therefore, an understanding of the operation of these protocols is essential in the context of forensic investigation. Network forensics is different from computer forensics since finding evidence can be more challenging. Usually data can be obtained from packet filters, intrusion detection systems and firewalls. However, attackers might circumvent such defenses by encrypting evidence, which indeed makes the investigator's task much harder.

Content Template	
Section Number	2.1.1
Section Title	Introduction
Introduction	This section provides an introduction to networking, discusses the importance of understanding networking principles and protocols for the network forensics investigator.
Content	For network investigators the number of potential sources of network-based evidence can be large. Therefore, understanding the operation of networking protocols is of high importance. Every communication environment needs special consideration from the network forensic investigator based on the relevant communication protocols. The investigator need always look at the network communication from different perspectives, and should expect to be confronted with previously unseen or new methods to hide evidence. This chapter reviews network service models and some important protocols, in addition to network tunneling in the context of network forensics. It discusses key protocols including IPv4, IPv6, IPsec, TCP, and UDP. This chapter is intended to provide the technical and conceptual foundation for later forensic-specific chapters.

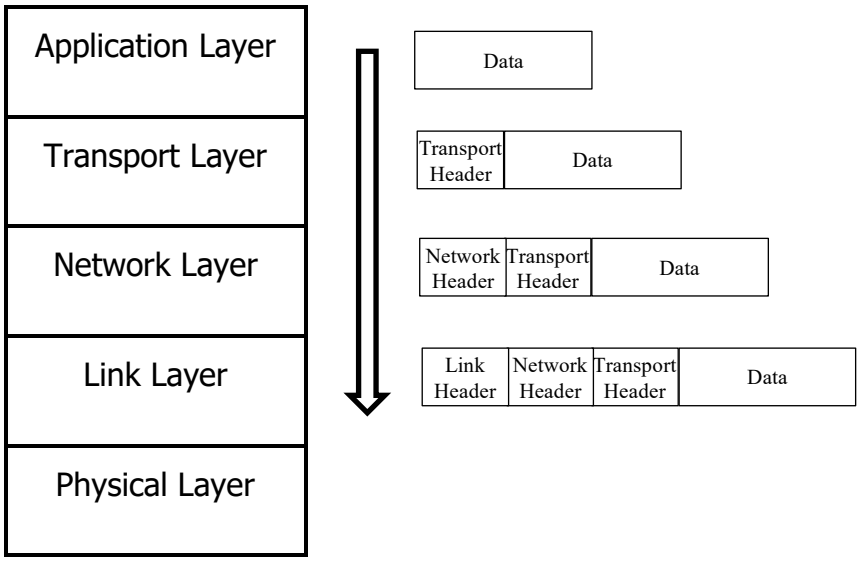
Content Template	
Section Number	2.2
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	In this section we will discuss two layered network models : The Internet protocol stack (also known as the TCP/IP stack) and the OSI model (Kurose & Ross, 2017). The Internet protocol stack consists of five layers as shown in Figure 2.1. Each layer supports functionalities through a collection of protocols. A network forensic investigator should be aware of the operation of these protocols in order to conduct an effective investigation. Forensic techniques usually rely on the understanding of these protocols, packet analysis and flow record techniques (Davidoff & Ham, 2012).  Figure 2.1: Internet protocol stack

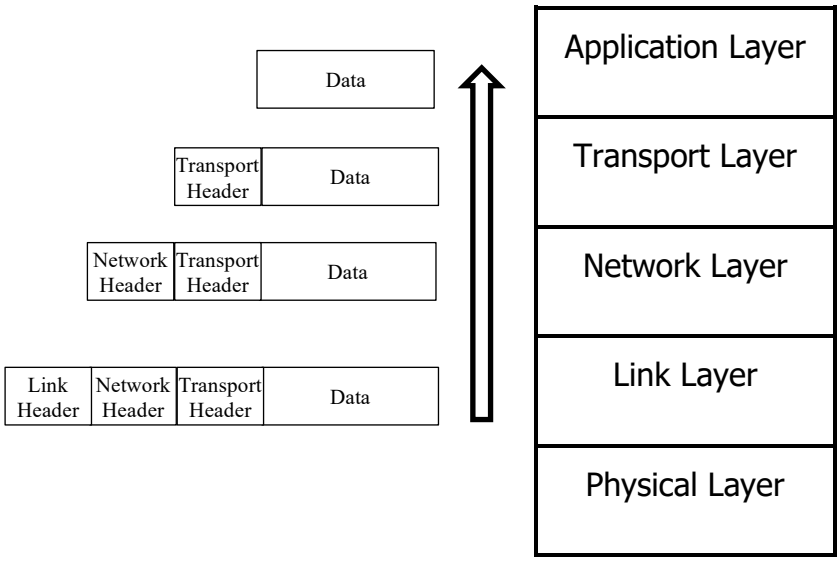
Content Template	
Section Number	2.2.1
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	For each of these layers there are protocols that are responsible for the services provided by each layer. An application layer protocol is responsible for supporting network applications in handling transmitted and received messages. For example, the HTTP or HTTPS protocols are used to support Web applications. Of course there are various application layer protocols such as SMTP, FTP, and many others, which facilitate the sending and receiving of messages on behalf of the application. By availing of such services , the application designer can focus more on the application itself rather than message handling . The network application may be loss-tolerant and not require a reliable transfer of the messages, or it might require reliable transfer . Therefore, the network application will specify the protocol that best fits its requirements in this regard. Such services are typically provided by the transport layer protocols, which are responsible for delivering data between end-to-end processes, i.e. client-server processes. There are two popular protocols that operate at the transport layer, namely TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Content Template	
Section Number	2.2.2
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	TCP provides reliable transport services while UDP is known as a best-effort protocol as it does not guarantee a reliable transfer of data. However, although UDP does not provide reliable transfer of data between processes, it is used for some very important network applications such as DNS and multimedia streaming. The network layer is responsible for delivering data between end systems (hosts). There are various protocols that operate at this layer such as Internet Protocol (IP) and routing protocols. routing protocols are responsible for building paths between end systems across the network nodes. A detailed discussion on routing protocols can be found in (Kurose & Ross, 2017). IP on the other hand facilitates the process of delivering data between hosts, section 2.3 focuses on IP. The link layer also participates in the process of delivering data, however, its main task is to deliver messages between neighboring network elements. link layer protocols such as Ethernet and 802.11 coordinate access to the communication link and deliver data frames between neighboring network elements. Once access to the link medium is granted the physical layer will transmit the data frame bits over the medium.

Content Template	
Section Number	2.2.3
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	The OSI model has two more additional layers, namely, the Session layer and the Presentation layer, which are located between the transport and the application layer. The session layer is responsible for establishing, managing and terminating the connections between end-to-end processes. The presentation layer on the other hand, is used to provide mapping of different syntax and semantics between application layer entities (Tanenbaum & Wetherall, 2010). **Encapsulation and decapsulation** When the network application process wants to communicate with a remote application process, it passes the message to the needed application layer protocol which formats it appropriately. The message is then passed to the layer below, which is the transport layer in this case. The transport layer encapsulates the message with the transport layer header to form a new message known as a segment and passes it to the network layer. The header contains the necessary information to deliver the original message to the appropriate process on the other side of the network.

Content Template	
Section Number	2.2.4
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	The network layer takes the segment and encapsulates it with the network layer header to form a new message named a datagram and passes it to the link layer. The header contains the necessary information to deliver it to the destination host. It is worth noting that the datagram network header is updated each time it is forwarded by a router over the path to the destination (time-to-live is decremented), however the transport layer is not affected and remains encapsulated. The link layer will also encapsulate the datagram with the link layer header and form a new message named a frame, which is then transmitted through the medium after gaining access for transmission. The link layer is updated as the frame traverses networks elements until it is delivered to the final destination. Figure 2.2 illustrates the whole process of encapsulation The process of decapsulation happens in the reverse order. So while the packet is traversing the network toward the destination it passes through network switches and routers. each of these devices can view and update the headers associated with the network layer at which they operate . A switch can view the link layer header and update its content accordingly. While in the case of a router it views and updates the headers of the link layer and network layer accordingly.

Content Template	
Section Number	2.2.5
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	 Figure 2.2: Encapsulation When the packet arrives at the final destination the link layer will decapsulate the frame by removing the link layer header and pass it to the network layer. the network layer removes its header and passes the segment to the appropriate transport layer since it has arrived at its final destination host. The transport layer in turn will remove its header and based on its contents will deliver the message to the appropriate process where it is handled by the application layer protocol. The process of decapsulation is illustrated in Figure 2.3.

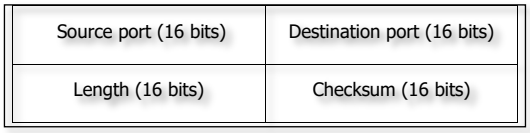
Content Template	
Section Number	2.2.6
Section Title	Network Protocol Stack
Introduction	In this section, we provide an overview of the network protocol stack. We discuss the Internet (TCP/IP) protocol stack and the OSI model
Content	 Figure 2.3: Decapsulation

Content Template	
Section Number	2.3
Section Title	**Internet Protocol**
Introduction	This section provides a brief review of the Internet Protocols IPv4 and IPv6
Content	The Internet Protocol (IP) is responsible for identifying hosts uniquely on the network using IP addresses and facilitates the process of routing data between the communicating hosts over the network. The data transmitted from the source is encapsulated with an IP header forming a packet (called a datagram above) which consists of both the IP header and the data coming from the transport layer embedded in the datagram payload. Because the payload is not fixed in size; the packet length is specified in its header. The packet is sent from the source to the destination by employing intermediate routers that utilize routing tables. These tables are created and updated through the use of routing protocols (Kurose & Ross, 2017). When a packet arrives at an intermediary router, some of header information, such as TTL and checksum, changes and fragmentation may occur. The first internet protocol is IPv4 which was standardized in 1981. It was designed with the end-to-end principle and is limited in functionality . Although IPv4 ensures an error-free packet header, (it calculates the checksum of the packet at the forwarding node), any corrupted packet is simply discarded. The receiving node is not required to notify the sender of this error.

Content Template	
Section Number	2.3.1
Section Title	**Internet Protocol**
Introduction	This section provides a brief review of the Internet Protocols IPv4 and IPv6
Content	However, if needed, another protocol supports such notification i.e. the Internet Control Message Protocol (ICMP) (Conta, Deering, & Gupta, 2006; Postel, 1981). IP does not support reliable end-to-end data delivery, sequencing, or flow control. Subsequently, in 1998 a new version was released named IPv6 to handle the address space limitation associated with IPv4 in addition to adding additional functionalities to the IP. It supports a larger address space by using 128 bits to represent the host IP address compared to only 32 bits in IPv4. IPv6, unlike IPv4, utilizes fixed length headers. It also provides network layer integrity and confidentiality by interoperating with IPsec.

Content Template	
Section Number	2.4
Section Title	**Internet Protocol Security (IPsec)**
Introduction	This section provides a description of IPsec, which is a network layer protocol that provides various functionalities including authentication, data integrity and confidentiality
Content	IPsec is a secure protocol suite popular in VPNs. It authenticates and encrypts the data packets sent over IP networks. The suite utilizes a group of protocols to establishing mutual authentication between nodes. IPsec provides various functionalities including network-level peer authentication, data integrity and confidentiality, and replay protection. Although security protocols usually operate at the application layer, IPsec operates at the network layer as an end-to-end security scheme, so it can secure applications at the network layer. It works well with both IPv4 and IPv6. The IPsec suite consists of the following important protocols: • The IP Authentication Header (AH) (Kent, 2005a), is used to guarantee data origin authentication and connectionless integrity of IP packets, by defining an optional packet header defending against replay attacks. • The IP Encapsulating Security Payload (ESP) (Kent, 2005b), provides various functionalities including confidentiality through encryption of the packet, data origin authentication, integrity protection, access control and also an optional protection against traffic analysis or replay attacks.

Content Template	
Section Number	2.4.1
Section Title	**Internet Protocol Security (IPsec)**
Introduction	This section provides a description of IPsec, which is a network layer protocol that provides various functionalities including authentication, data integrity and confidentiality
Content	• The Internet Key Exchange (IKE) (Kaufman, Hoffman, Nir, Eronen, & Kivinen, 2014) protocol allows hosts to identify the services to be incorporated in packets, and hence, aids in selecting the appropriate cryptographic algorithms to provide these services and the required key sharing mechanism. IPsec operates in in two modes which are described as follows: • Transport mode: The IPsec encapsulates only the payload of the IP packet. The original IP header remain intact, except the IP protocol field. • Tunnel mode: In this mode the entire packet contents including the IP header and its payload are encrypted and then with a new IP header, the entire packet is encapsulated.

Content Template	
Section Number	2.5
Section Title	**User Datagram Protocol**
Introduction	This section discusses the operation of UDP
Content	The User Datagram Protocol (UDP) is an important protocol for many network applications. Despite it being an extremely simple and light weight protocol. UDP is a connectionless protocol and it does not provide any special services to the network application such as reliable data transfer, flow control or congestion control. Such protocol is useful for applications that are loss-tolerant and require fast transmission of data such as multimedia streaming. Another attractive facet in the design of the protocol is its small header size of eight bytes , shown in Figure 2.4. The source and destination port numbers represent the port number of the sending and receiving processes. It is important to note that, being connectionless, with UDP; the process socket is identified using a tuple of two values; the destination IP address and destination port number. Thus, if two segments arrive from a different source address or source port number but have the same destination address and destination port number then these segments will be directed to the same process. The checksum is used for error detection. Finally, the length represents the size of the segment in bytes including the UDP header.  Figure 2.4: UDP header format

Content Template	
Section Number	2.6
Section Title	**Transmission Control Protocol**
Introduction	This section describes the main operation of TCP
Content	TCP is a transport protocol that provides reliable end-to-end data transfer between application processes. It is a connection-oriented protocol that provides both flow control and congestion control. TCP supports various applications that require reliable data delivery such as Web applications, email, file transfer and many others. Figure 2.5 illustrates the TCP header fields. The header has a minimum length of 20 bytes representing the mandatory fields in the header. The optional options field can be up to 40 bytes in length. Following is a brief description of some of these fields: • Source port and Destination port numbers: These fields represent the port number of the sending process and the port number of the receiving process. It is important to note that with TCP since it is connection-oriented, the process socket is identified a tuple of four, the source IP address, source port number, destination IP address and destination port number. • Sequence number: this represents the byte sequence sent in the current segment . • Acknowledgment number: This represents the next sequence number that the receiver is awaiting to be sent by the sender. The receiver uses this to request the next segment and to acknowledge the received ones.

Content Template	
Section Number	2.6.1
Section Title	**Transmission Control Protocol**
Introduction	This section describes the main operation of TCP
Content	• Window size: This field is used for flow control and it represents the amount the receiver is willing to take in bytes. • Header length: this represents the size of the header in 32-bit units. • Checksum: This is used for detecting errors. • Urgent pointer: This represents where the urgent data ends from the sequence number and it is used only if the urgent flag is set.

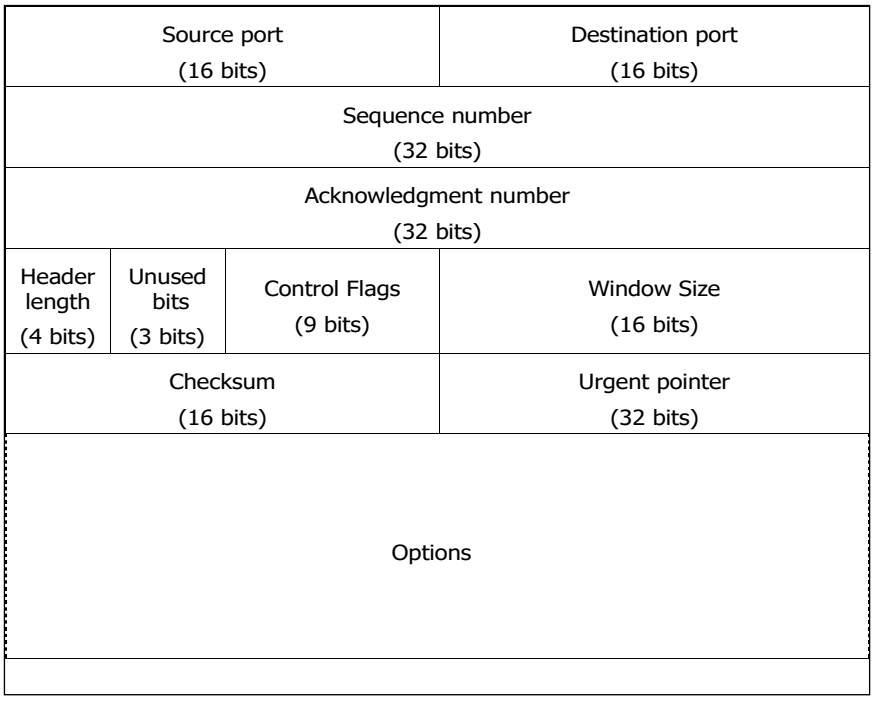


Figure 2.5: TCP header format

Content Template	
Section Number	2.7
Section Title	**Network Tunneling**
Introduction	This section introduces network tunneling
Content	Although IPv6 was released in 1998, many networks are still operating on IPv4. Therefore, in order to pass traffic between these networks we use tunnels. This is done by encapsulating IPv6 packets in UDP packets transmitted through IPv4. Because of the complexity of the transition from IPv4 to IPv6, there are many protocols to support the IPv6 transition (Nordmark & Gilligan, 2005) . Organizations may use tunnels to connect various locations while keeping traffic protected and confidential. Tunneling can be used to remotely access private networks. Internet Protocol Security (IPsec) is a protocol that can facilitate tunneling by building a virtual private network (VPN). Of course, there are other ways to securely accessing private networks by using cryptographic protocols such as TLS and SSH, which encrypt traffic and hence provide confidentiality. Tunneled traffic may challenge the forensic investigator when inspecting traffic between remote sites when the investigator has no access to the communicating devices and has to collect evidence from the packets traversing the network. with the help of the network administrators the investigator can gain access to these packets.

Content Template	
Section Number	2.7.1
Section Title	**Network Tunneling**
Introduction	This section introduces network tunneling
Content	For example, if the traffic was IPsec encapsulated, the investigator can recover the source and destination addresses. However, if the packets were encrypted the investigator will need to recover the packets from the transport layer to bypass the tunneling protocol. It is worth noting that there are many methods to perform traffic tunneling such as: covert tunneling, TCP sequence numbers, DNS tunnels, and ICMP tunnels. For details on these tunneling methods please refer to (Davidoff & Ham, 2012).

Activity Template	
Number	2.1
Title	Security Attacks no TCP/IP Suit Layers
Type	Reflection
Aim	Acquire a basic knowledge about common attacks on the different TCP/IP suit layers.
Description	For each layer of the TCP/IP suit, write about two possible security attacks that specifically target this layer.
Timeline	1 Hour
Assessment	The student should submit a written report. The instructor grades the report as follow: Each TCP/IP layer: 20%, each attack 10%

Activity Template	
Number	2.2
Title	IPsec security protocol
Type	Review
Aim	Understand the importance of the IPsec security protocol. Besides, understanding how IPsec operates.
Description	Write a report about three different attacks that the IPsec protocol can mitigate. Describe how using IPsec avoids these security attacks.
Timeline	2 Hour
Assessment	The student should submit a written report. The instructor grades the report as follow: Tools assessment: 90%, for each attack 30% Overall work: 10%

Activity Template	
Number	2.3
Title	Covert Tunneling
Type	Research
Aim	Inspect covert tunneling techniques, which may be used as a dangerous tool for data exfiltration.
Description	Study two known attacks of covert tunneling and explain the steps of these attacks and the reason of their success.
Timeline	2 Hour
Assessment	The student should submit a written report. The instructor grades the report as follow: The tunneling attacks: 40%, for each attack 20% Explaining the steps: 40%, for each attack 20% Determining the reason of their success: 20%, for each attack 10%

Think Template (MCQs)	
Number	2.1
Title	Network Protocol Stack
Type	Choose the correct answer
Question	The layer that is responsible for delivering data between end systems (hosts) is: a) Transport Layer b) Network Layer c) Link Layer d) Application Layer
Answers	The correct answer is (b)

Think Template (MCQs)	
Number	2.2
Title	Network Protocol Stack
Type	Choose the correct answer
Question	A packet transitions the complete protocol stack at: a) Sending host b) Receiving host c) Router d) Both (a) and (b)
Answers	The correct answer is (d)

Think Template (MCQs)	
Number	2.3
Title	Internet Protocol
Type	Choose the correct answer
Question	IPv4 provides the following services: a) reliable end-to-end data delivery b) error notification c) flow control d) None of the above
Answers	The correct answer is (d)

Think Template (MCQs)	
Number	2.4
Title	User Datagram Protocol
Type	Choose the correct answer
Question	The User Datagram Protocol (UDP) is one of the important protocols that serves a wide range of vital network applications. It provides the following services: a) Reliable data transfer b) Flow control c) Congestion control d) None of the above
Answers	The correct answer is (d)

Think Template (MCQs)	
Number	2.5
Title	Transmission Control Protocol
Type	Choose the correct answer
Question	TCP header consists of mandatory and optional fields. The header length is : a) 8 bytes b) 20 – 40 bytes c) 60 bytes d) 1024 bytes
Answers	The correct answer is (b)

Extra Template	
Number	2.1
Title	Computer Networking: A Top-Down Approach
Topic	1. Computer networks and the internet
Type	Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach (7 ed.): Pearson. ISBN: 0132856204

Extra Template	
Number	2.2
Title	Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification
Topic	2. ICMPv6 (ICMP for IPv6)
Type	Conta, A., Deering, S., & Gupta, M. (2006). Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification. RFC 4443: IETF.

Extra Template	
Number	2.3
Title	Basic transition mechanisms for IPv6 hosts and routers
Topic	3. Configured Tunneling Mechanisms
Type	**RFC article:** Nordmark, E., & Gilligan, R. (2005). Basic transition mechanisms for IPv6 hosts and routers, RFC 4213: IETF.

Extra Template	
Number	2.4
Title	Internet key exchange protocol version 2 (IKEv2)
Topic	1. Introduction
Type	**RFC articles:** Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). Internet key exchange protocol version 2 (IKEv2), RFC 7296: IETF.

Extra Template	
Number	2.5
Title	Network Forensics: Tracking Hackers through Cyberspace
Topic	11. Network Tunneling
Type	**Book:** Davidoff, S., & Ham, J. (2012). Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall. ISBN: 0132565102

Extra Template	
Number	2.6
Title	Computer Networks
Topic	14. Reference models
Type	Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5 ed.): Pearson. ISBN: 0132126958

Extra Template	
Number	2.7
Title	Internet control message protocol
Topic	1. Introduction
Type	**RFC articles:** Postel, J. (1981). Internet control message protocol, RFC 792: IETF.

Extra Template	
Number	2.8
Title	Internet key exchange protocol, IP Authentication, and IP encapsulating security payload
Topic	2. Encapsulating Security Payload Packet Format
Type	**RFC articles:** Kent, S. (2005a). Header, IP Authentication. RFC 4302 (Vol., RFC 4302): IETF.

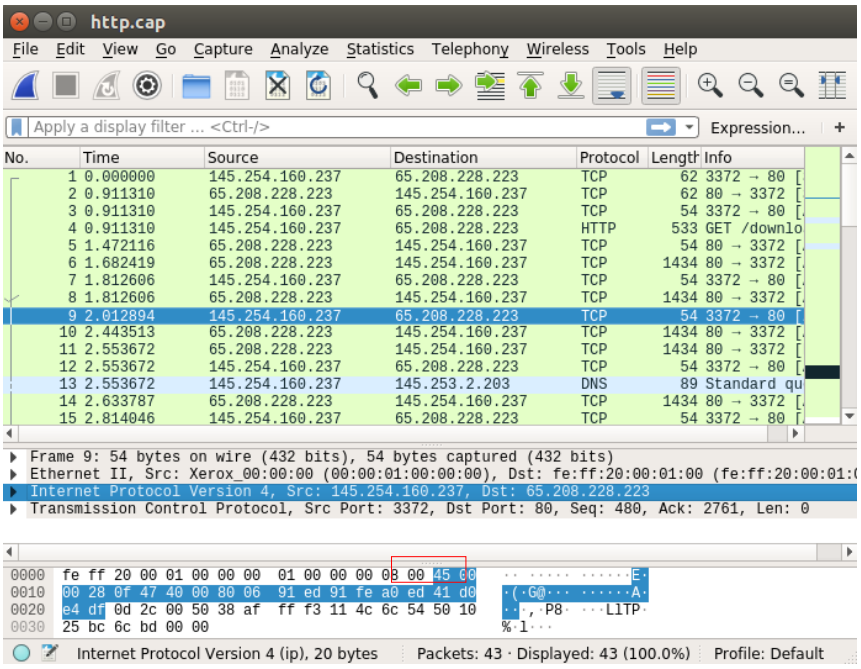
Extra Template	
Number	2.9
Title	IP encapsulating security payload (ESP)
Topic	1.1 Overview
Type	Kent, S. (2005b). IP encapsulating security payload (ESP), RFC 4303: IETF.

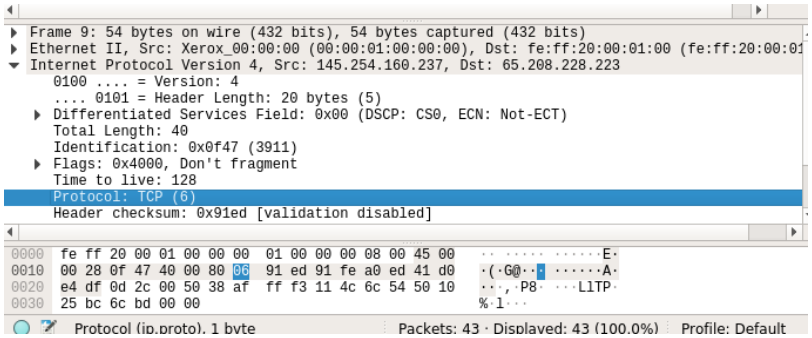
3. Traffic Analysis

Scope Template	
Number	3
Title	Traffic Analysis
Introduction	This chapter covers the basic skills and concepts required to understand and practice network traffic analysis. These skills are Protocol Analysis, Packet Analysis, and Using Packet Sniffer and Analysis Tools and Flow Analysis.
Outcomes	After the completion of this chapter, the student will be able to demonstrate fundamental traffic analysis skills, including protocol and packet analysis. The student will be able to apply packet analysis tools to extract information of interest, specifically; the student will learn the basics of using the Wireshark tool.
Topics	4. Traffic Analysis 1. Network Traffic Analysis 2. Protocols Analysis i. Protocol Analysis Steps 3. Packet Analysis i. Capture Packets using Wireshark ii. Packet Analysis using Wireshark iii. Packet Analysis Techniques 4. Flow Analysis i. Flow Analysis using Wireshark ii. Flow Analysis Techniques 5. Challenges of traffic analysis
Study Guide	• Required study time. ○ 12 hours • Required hardware/software. ○ Wireshark • Required external resources including links and books. ○ Network Forensics: Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012, ISBN: 0-13-256471-8. ○ Practical packet analysis: Using Wireshark to solve real-world network problems, 3rd Edition. Sanders, Chris. No Starch Press, 2017, ISBN: 978-1-59327-802-1.

Content Template	
Section Number	3.1
Section Title	Network traffic analysis
Introduction	This section covers the definition of traffic analysis, how it is different from traditional Hard Disk/persistent storage media analysis and the basic skills required for conducting traffic analysis.
Content	Traffic analysis is defined as the process of capturing and analyzing data that flows within the network with the aim of extracting useful information. This information can help the investigator identify suspicious traffic such as data smuggling or help the network administrator find a complex configuration error in a router. On the other hand, attackers use traffic analysis to locate any weakness or vulnerability that can help them break into the network. Network traffic analysis is different from traditional hard disk analysis: network traffic is constantly changing and the volume of traffic that passes through the network is unlimited. traffic analysis requires several skills such as being able to interpret packet structure, familiarity with different protocol types and how they operate, and most importantly the ability to isolate, and analyze a specific flow of packets. To conduct a traffic analysis efficiently, several tools and techniques are required. The most prevalent are Wireshark, tcpdump and Tshark. However, the tools must be chosen carefully, since the specification and protocols of the underlying network are constantly changing, thus tools should be updated and changed accordingly.

Content Template	
Section Number	3.2
Section Title	Protocol Analysis
Introduction	Traffic analysis starts with an understanding of network protocols. This section covers the concept and importance of protocol analysis.
Content	Network protocols are a set of rules and procedures that regulate the communication between two entities. These protocols are designed to work at the different network layers. protocol analysis is the process of identifying the protocol types, how they operate and analyzing them. Protocol documentation provides the main source to understanding protocol operation and structure. The most well-known source of protocol documentation is the IETF's public repository and there are other standards organizations such as IEEE-SA and ISO that provide further protocol documentation. Vendors such as CISCO and Microsoft also provide protocol documentation. In addition, researchers may also publish protocol documentation. However, many protocols' documentation may be kept secret by their inventors.

Content Template	
Section Number	3.2.1
Section Title	Protocol Analysis Steps
Introduction	This section covers the main protocol analysis steps. the first step is protocol identification including searching the packet for a specific signature associated with the protocol.
Content	Protocol analysis requires deep understanding and experience, however, for now the student needs to know the three main steps and then you can expand your experience by working on more examples. These steps are protocol identification, protocol decoding and exporting protocol fields. **Protocol Identification** The first step in protocol analysis is to identify the used protocol in the captured traffic. You can do this by (1) searching for a specific signature associated with the protocol such as known hexadecimal, binary or ASCII values. An example of such signature is the hexadecimal sequence at the beginning of IPv4 packets, which always start with "0x4500" as shown in the Figure 1.  Figure 1: A screenshot of Wireshark program; we will talk about in this tool in details in section 3.3.3 This is a screenshot of Wireshark program which is discussed further in section 3.3.3

Content Template	
Section Number	3.2.2
Section Title	Protocol Analysis Steps
Introduction	This section covers the main protocol analysis steps; the first step is the protocol identification including searching the packet for useful information, using port number, identify the function of the communicated entities or packet dissect.
Content	(2) protocol type may also be determined using information within the protocol fields. For example, in network packets, the protocols in lower-layers contain information about protocols in higher-layers (in order to support demultiplexing). In the figure below, the "Protocol" field in IP packet contains the type of higher layer protocol. Figure 2 indicates that the upper layer protocol is TCP.  Figure 2: The details of protocol layer fields in network packet. (3) Using the port number (TCP or UDP). We can determine the protocol from the used port number, i.e., standard services are associated with a predefined port number. For example, the FTP uses TCP port number 21 for communication. (4) We can also know the protocol if we can identify the function of any of the communication entities (using their IP address or hostname). (5) If none of the previous steps worked, you need to dissect the packet in attempt to identify any known protocol structure. This relies on an understanding of common header values and protocols structure; in this case, testing for the existence of a particular protocol within the captured packets is advised.
Content Template	
Section Number	3.2.3
Section Title	Protocol Analysis Steps
Introduction	This section covers the main protocol analysis steps, after determining the protocol type; the next step may be packet decoding and then exporting fields.
Content	**Protocol Decoding:** Bits within the packet fields contain information that are used to regulate the communication, describe the protocol itself or describe higher-layer protocols and their payload. The protocol decoding is used to interpret these bits according to a defined protocol structure. Commonly, protocol decoding is performed using analysis tools, which saves time and resources . However, you can write a decoder or manually decode the traffic according to a public documentation.

Exporting Fields: Finally, after decoding the packet fields you just need to export its contents and you can easily do this using Wireshark.

Tools such as Wireshark, automatically decodes and interprets the packet contents, in figure 3 we can see the TCP protocol fields using Wireshark.

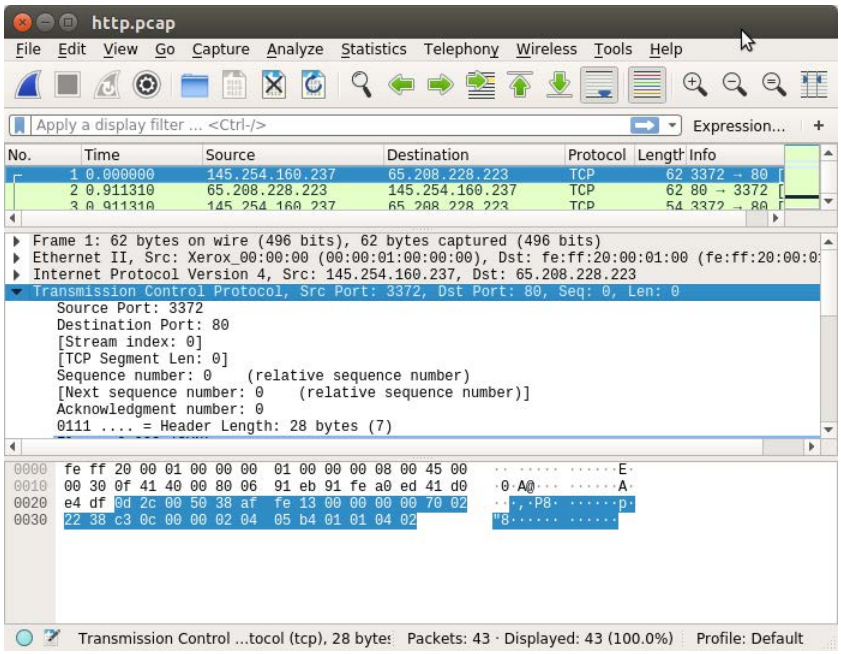
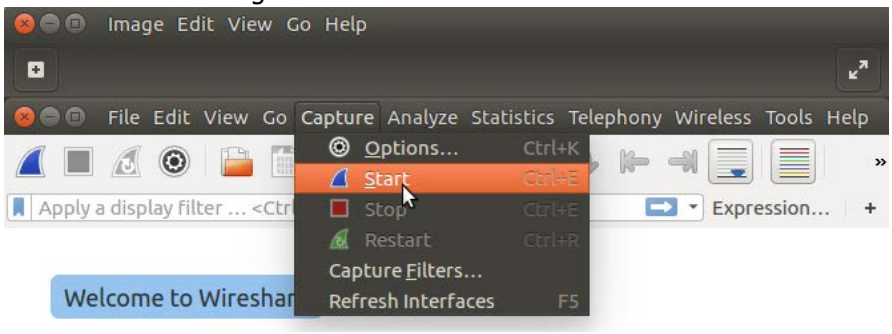
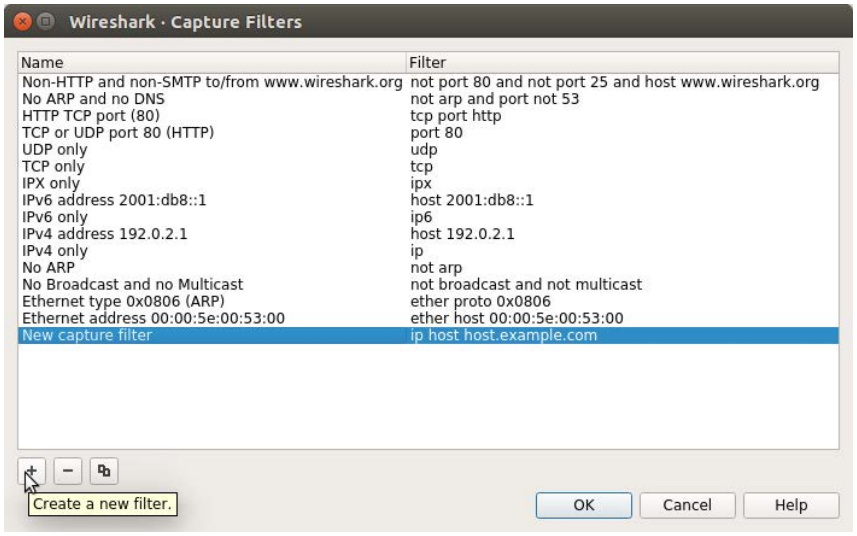


Figure 3: TCP protocol fields.

Content Template	
Section Number	3.3
Section Title	Packet Analysis
Introduction	This section describes packet analysis and the importance of filtering packets of interest. The student will be able to perform high level analysis of traffic.
Content	The data travelling between two communicating network entities is held in packets whose structure is determined by protocols. In network forensics, packet analysis is conducted to identify relevant packets, expose their structure and illuminate the relationship between packets to build evidence. Relevant packets can be identified based on a particular pattern or string within packets or based on protocol fields . Packet analysis is fundamental to reconstructing communication, transferred files and other flows in the network. It helps uncover malicious activities, possible attacks, vulnerabilities in applications and manage the network. To start packet analysis, live data may be captured while it flows through the network or a pre-existing packet capture may be employed. A packet sniffer is used For capturing network packets .

Content Template	
Section Number	3.3.1
Section Title	Packet Capture using Wireshark
Introduction	This section describes packet capture using Wireshark . The student will learn to capture packets using Wireshark tool.
Content	The most well-known packet analysis tool is Wireshark, which contains built-in dissectors for a large number of protocols. It automatically interprets protocol fields within packets and has a user-friendly interface that makes the protocol analysis an easier task. Wireshark is an open source tool that can be downloaded from its website: https://www.wireshark.org/download.html Wireshark can be used for live traffic or capture or to analyze existing pcap files. Once installed, packet capture is initiated by choosing "Capture" → "Start" as shown in figure 4.  Figure 4: Capture menu in Wireshark. Choose "Stop" to finish capturing the packets. captured traffic can then be saved in pcap format (*.pcapng) using "File" → "Save As". From "Capture"→ "options", it is possible to select between the different network interfaces on which to perform the capture. Before capturing packets, we need to ask: What is the goal of capturing packets? What will we capture? And what is the flow of these packets? The answer to these three questions can help to avoid capturing large number of irrelevant packets.

Content Template	
Section Number	3.3.2
Section Title	Capture Packets using Wireshark
Introduction	This section introduces how to capture packets based on a specific capture filter using Wireshark tool.
Content	Once the structure or content of relevant packets has been , "Capture Filters" can be applied to restrict the capture to just those packets  Figure 5: A predefined filters list defined by Wireshark As shown in in figure 5, predefined filter types can be extended with a new capture filter by clicking on the "+" button. filters can be built based on (1) The host IP address: "host 192.0.2.1", which means to only capture packets that include this IP address as source or destination (2) port number: "port 8080", means to capture only packets with port number 8080 as source or destination. "!port 8080", means to capture any packet except the ones that include 8080 as port number for source or destination. (3) Protocol type: "tcp", only capture tcp traffic. (4) Protocol fields: icmp[0] == 8, only capture icmp packets of type "echo request message". (5) Combination of filters: not arp and port not 53, means capture all traffic except ARP and DNS (port 53) packets. Capture filters are very handy to avoid capturing a large volume of irrelevant packets. However, care should be taken in choosing the correct filter type so important traffic will not be missed.

Content Template	
Section Number	3.3.3
Section Title	Packet Analysis using Wireshark
Introduction	This section introduces the Wireshark interface including the packet list pane. The student will be familiar with the Wireshark too interface.
Content	Using Wireshark, packet content and details of supported protocols can be viewed or even a new packet dissector can be created and added within Wireshark. Figure 6 contains the "NTP_sync.pcap" file. The main window of Wireshark has three panes:

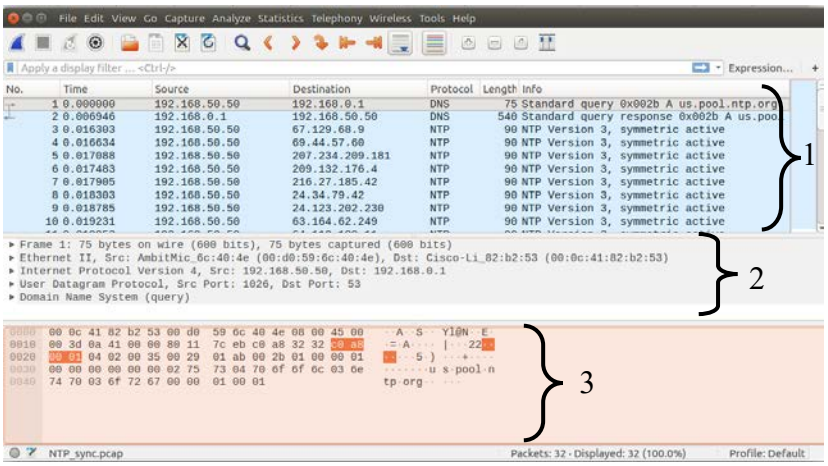


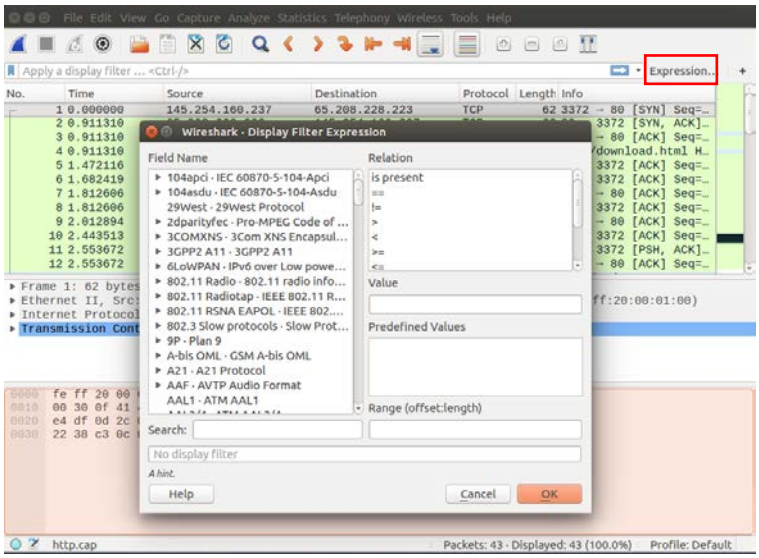
Figure 6: The main window of Wireshark

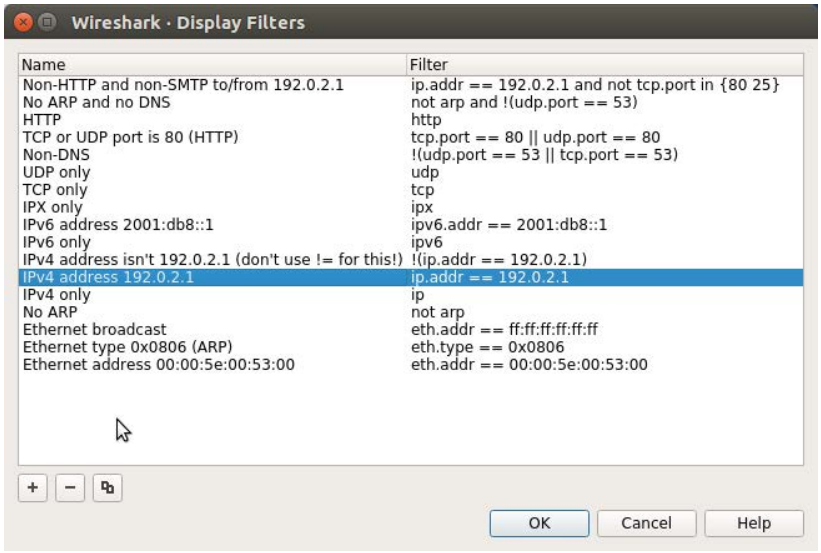
1. Packet List:

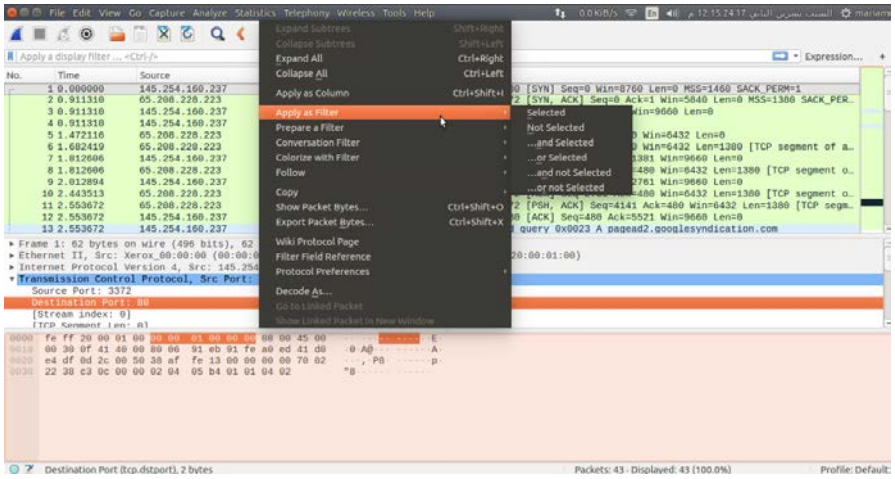
This panel displays captured packets, each packet appears in one line with brief information about this packet. The information includes: (1) The sequence number of the packet in the capture file. (2) Timestamp indicating when the packet was captured. (3) Source IP address of the packet. (4) The destination IP address of the packet. (5) The highest-level protocol in the packet. (6) The length of the packet. (7) brief information about the contents of the packet.

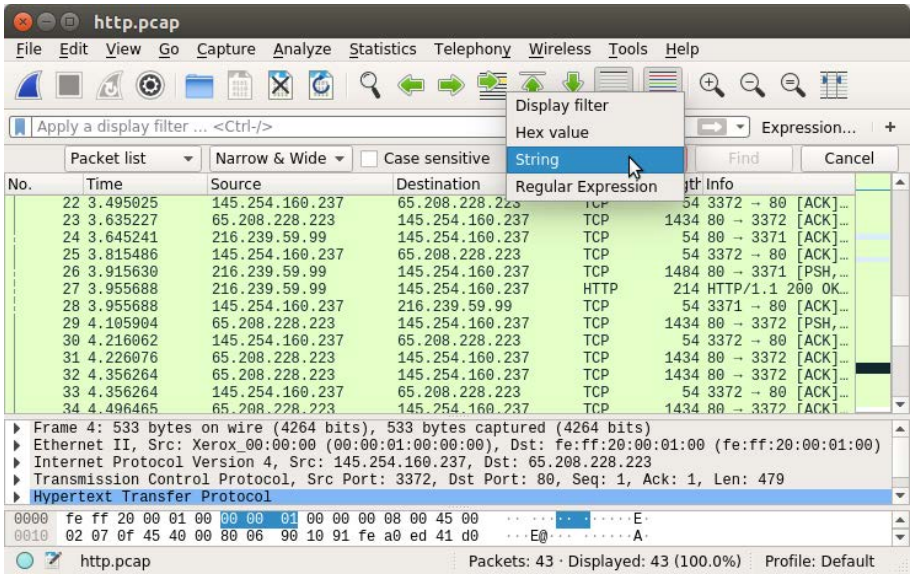
Clicking on any line in this pane, will display the selected packet in more detail in the "Packet Details" and "Packet Bytes" panes.

Content Template	
Section Number	3.3.4
Section Title	Packet Analysis using Wireshark
Introduction	This subsection introduces the Wireshark interface including the packet details and packet bytes panes.
Content	**2. Packet Details:** This pane shows the structure of all captured packets including component fields in a tree form arranged according to network layer number. **3. Packet Bytes:** Displays the data of the selected packet from the packet list in hexadecimal and ASCII representations. Each line shows the offset of the data, sixteen hexadecimal bytes along with their corresponding ASCII bytes. A period (".") will appear instead of any non-printable byte. Wireshark automatically chooses a protocol dissector to use for a specific packet. For packets that require using a different protocol dissector, use Wireshark's "Analyze→Decode As" function to modify the dissector in use.

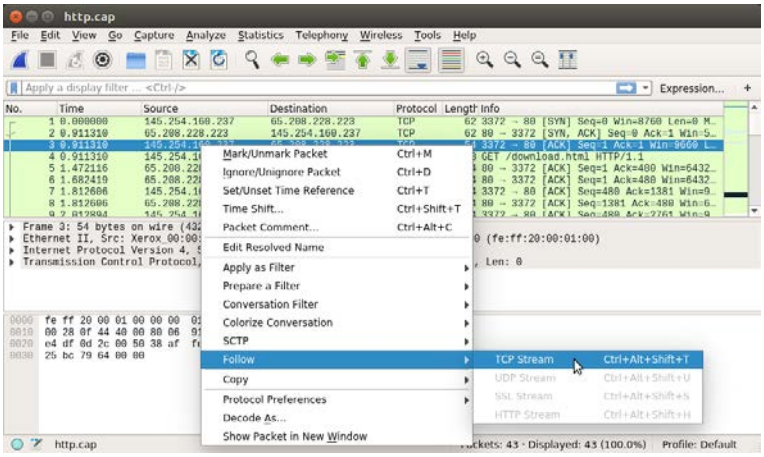
Content Template	
Section Number	3.3.5
Section Title	Packet Analysis using Wireshark
Introduction	This subsection covers the steps of packet filtering using the expression button.
Content	Filtering relevant packets is one of the more powerful features of Wireshark; by using the "display filter", relevant packets v=can be isolated based on protocol fields. The display filter can be applied on more than 227,000 fields of 3,000 protocols in Wireshark 2.6.3 and this number is only set to increase as new protocol parsers are added. In addition, new protocol parsers can be written and added as a plugin to Wireshark. The difference between capture filter and display filter, is that display filter, filter packets already captured and saved. In the Filter Toolbar, use the "Expressions" button (red rectangle) to define a filter.  Figure 7: Using expressions to define capturing filters. Figure 7 above shows the "http.cap" file.

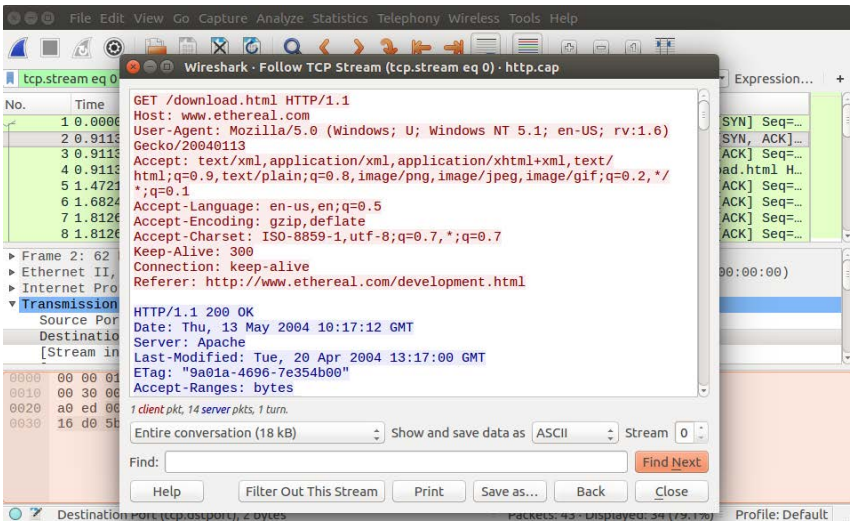
Content Template	
Section Number	3.3.6
Section Title	Packet Analysis using Wireshark
Introduction	This section covers the steps of packet filtering using the menu choice "Analyze" → "Display Filters".
Content	 Figure 8: Display filters of Wireshark. can also apply a display filter using the "Analyze" → "Display Filters" menu choice. display filters are similar to capture filters; see Figure 8, however, their syntax is slightly different. A Display filter can be applied on: (1) The host IP address: "ip.addr==192.0.2.1", which means to only display packets that include this IP address as source or destination (2) port number: "tcp.port == 8080", means to display only packets with port number 8080 as source or destination. "!(tcp.port == 8080)", means to display any packet except the ones that includes 8080 as port number for source or destination. (3) Protocol type: "tcp", only display tcp traffic. (4) Combination of filters: tcp.port == 80 || udp.port == 80, means display only packets with tcp or udp traffic with port number 80.

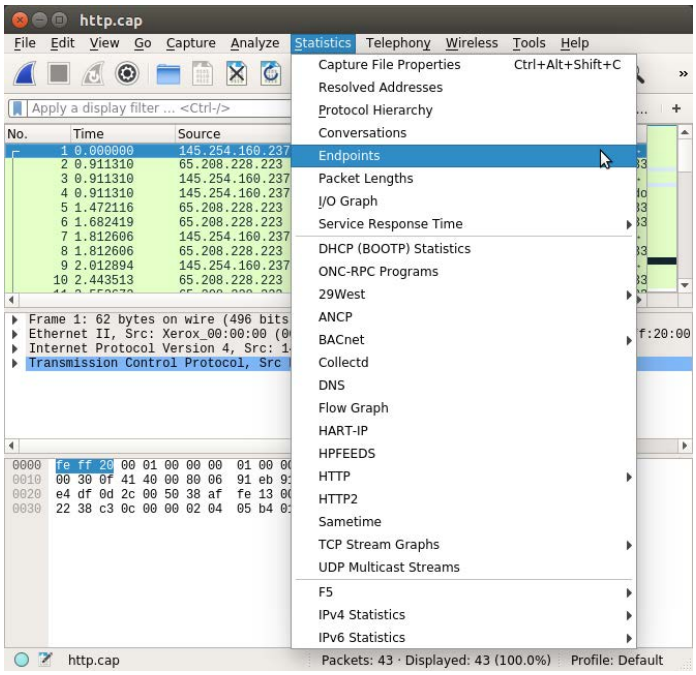
Content Template	
Section Number	3.3.7
Section Title	Packet Analysis using Wireshark
Introduction	This section covers the steps of packet filtering based on a selected packet within the capture traffic. The student will be able to apply packet filtering using Wireshark based on specific packets in the capture.
Content	An alternative to manual display filter specification is to , right-click on any filed in the "Packet Details" window and choose "Apply As Filter", as shown in Figure 9, which will set the filter based on that fields' value.  Figure 9: Applying Wireshark filter using a selected packet.

Content Template	
Section Number	3.3.8
Section Title	Packet Analysis Techniques
Introduction	This subsection covers the steps of packet analysis including pattern matching, parsing protocol fields and packet filtering. The student will learn to analyze packets based on pattern matching, parsing protocol fields or packet filtering
Content	Packet analysis main techniques are: (1) Pattern Matching: Identify relevant packets by searching for a specific value within the packet structure. (2) Parsing Protocol Fields: Export bits within protocol fields. (3) Packet Filtering: Filter packets according to a specific field value in the protocol payload or metadata. Can be conducted using Wireshark display filters. In order to find a specific packet of interest choose the "Find Packet" option from the "Edit" menu, Figure 10, which will display the search tab. then search the packets based on a display filter, hex value or string within the packet. use a regular expression to search on multiple packets at the same time.  Figure 10: Using "find Packet" option in Wireshark.

Content Template	
Section Number	3.4
Section Title	Flow Analysis
Introduction	This section introduces the concept of flow analysis.
Content	Flow analysis refers to the process of studying groups of related packets in order to extract useful information such as traffic patterns and suspicious activity. flow analysis, sometimes called data stream analysis, helps to reconstruct events, transferred files, transactions and conversations that span more than one packet in the stream. flow analysis starts by determining the flow of interest within the traffic capture based on a specific filter or characteristic. Subsequently , this flow can be isolated for further investigation. Finally, data or files can be extracted from the flow.

Content Template	
Section Number	3.4.1
Section Title	Flow Analysis using Wireshark
Introduction	This section covers the steps of conducting flow analysis using Wireshark on a TCP flow.
Content	In Wireshark, a flow is named a "conversation", which may contain TCP, UDP or IP traffic between two particular endpoints. Any flow (conversation) can be displayed in a packet capture, by isolating the selected flow and saving it for further analysis, where data or files (file carving) from the selected flow can be extracted. Wireshark has built-in capabilities to filter, reconstruct and export network flows. For example, the "Follow TCP Stream" function enables the reconstruction of the contents of a stream automatically using any packet within the TCP stream. Right click on the packet of interest in the "Packet List" and choose "follow" → "TCP Stream", as shown in Figure 11. The "TCP stream" combines data that spans different packets from protocols that use TCP, such as HTTP and FTP.  Figure 11: Steps of TCP stream reconstruction.

Content Template	
Section Number	3.4.2
Section Title	Flow Analysis using Wireshark.
Introduction	This section covers the steps of conducting flow analysis by showing the conversation between two entities.
Content	By choosing a specific TCP stream, a new window that contains the conversation contents will pop up. This conversation can be saved in several forms and each side of the conversation can be saved separately.  Figure 12: Content of TCP conversation. In the above conversation, we can see the TCP communication, starting with an initial HTTP "GET" request from the client and a successful response from the server containing a "HTTP/1.1 200 OK" message. repeated patterns are observable within this stream as the client requests additional files and the server responds by sending them.

Content Template	
Section Number	3.4.3
Section Title	Flow Analysis using Wireshark
Introduction	This section introduces the concept of statistical analysis using Wireshark.
Content	In some contexts, flow analysis refers to the statistical analysis of packet flow or metadata flow. statistical analysis is used to analyze the traffic even if encrypted (and cannot be decrypted). If the traffic was encrypted, the statistical analysis can reveal important information such who are the communicating entities, their locations, time of sending packets and the pattern and volume of communication. In such cases, the larger volume of traffic captured the better the information obtainable . Clicking on the "Statistics" menu option, reveals several options such as "Endpoints".  Figure 13: Statistics menu option to display specific packets.

Content Template	
Section Number	3.4.4
Section Title	Flow Analysis using Wireshark
Introduction	This section introduces the concept of statistical analysis using Wireshark.
Content	Choosing Endpoints, the following window will appear showing the number and length of packets between the communicating endpoints.

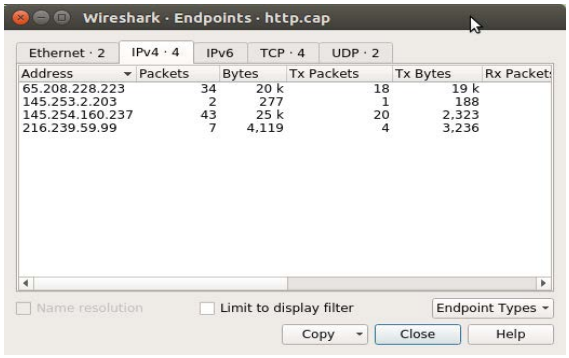


Figure 14: Endpoints statistics using Wireshark.

Another important option in the "Statistics" menu is the protocol hierarchy, which shows the most used protocols between two entities.

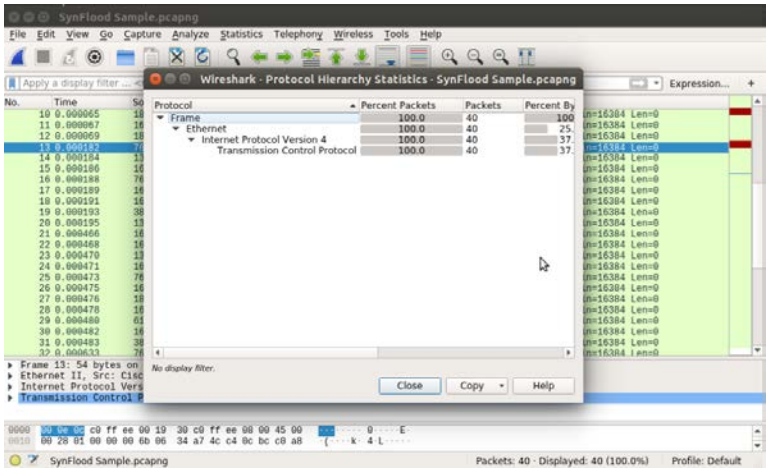


Figure 15: Protocol Hierarchy Statistics using Wireshark.

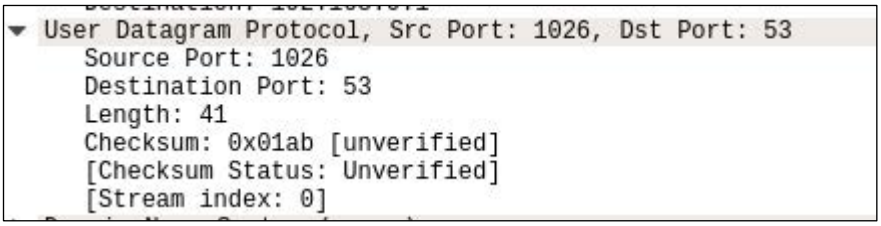
Figure 15 displays the file "SynFlood Sample.pcapng". The SYN Flood attack sends TCP SYN packets without replying to the server's SYN-ACK in order to check if a specific port is open or to flood the server with half-open connections thereby denying service to legitimate clients.

Content Template	
Section Number	3.3
Section Title	Traffic Analysis Challenges
Introduction	This section covers network traffic analysis challenges.
Content	traffic analysis is not a straightforward task and requires many skills and experience. common challenges are as follows: • The loss, truncation or corruption of packet contents or protocol information. • Encrypted packet contents: the contents of the packet may be encrypted at different network layers. • Undocumented protocols: Many protocols have no documentation, either to preserve communication security or to maintain intellectual property rights. Simply, some protocols may have weak documentation due to a lack of resources . • Although some protocols are documented, this does not mean that they were implemented correctly as described in their specification. Attackers take advantages of this fact to hide data in unused fields, bypass firewalls and IDSs. • Data hiding and covert communication techniques: data hiding techniques vary in their types and methods. For instance, attackers create new protocols or add an extension to old ones in order to communicate secretly. • Large traffic volumes: currently IoT and big data frameworks produce a large volume of data that makes the acquisition of all data challenging or in many cases impossible to achieve • When the volume of traffic is very large it is difficult to determine the packets relevant to the analysis. • The complexity of packet analysis tools is a challenge for newcomers to the field.

Activity Template	
Number	3.1
Title	Analyze Network Protocols
Type	Review
Aim	Upon completion of this activity students will be able to discriminate between different protocol types based on their structure.
Description	Choose two protocols from each of the following layers: Application, Transport and Network. For each protocol draw the protocol (i.e. packet header) structure and determine the main feature that can be used to identify this protocol in a packet capture.
Timeline	1 Hour
Assessment	The student should submit a written report. The instructor grades the report as follows: Protocol Structure: 60%, 6 x each protocol 10% Protocol Features: 30%, 6 x each feature 5% Overall work: 10%

Activity Template	
Number	3.2
Title	Analyze Port Scanning Attack
Type	Reflection
Aim	Upon completion of this activity students will be able to use Wireshark to analyze a real attacks
Description	Search the Internet for three samples of port scanning attacks (.pcap files), open these files using Wireshark and study them. Your task is to extract the main features, patterns or signature contained in these attacks.
Timeline	30 minutes to search the Internet 1 hour to explore the data 1 hour to write the report Total: 2 hours and 30 minutes
Assessment	The student should submit three pcap files (contains port scanning attacks) and a written report. The instructor grades the activity as follows: Selection of the pcap files: 30% Report: 60%, for each feature of attack 3 x 20% Overall work: 10%

Activity Template	
Number	3.3
Title	Features of Packet Analysis Tools
Type	Research
Aim	The student will be gain the skill of using packet analysis tools and understand how these tools work.
Description	Write a report detailing the comparative features, capabilities and deficiencies of each of the following packet analysis tools: *Wireshark*, *tcpdump* and *tshark*. As a conclusion to your report, emphasize the difference between these three tools in a table.
Timeline	5 hours
Assessment	The student should submit a written report. The instructor grades the report as follow: Tools assessment: 60%, for each tool 3 x 20% Conclusion: 40%

Think Template (MCQs)	
Number	3.1
Title	Protocol Analysis
Type	Choose the correct answer
Question	Regarding the following snapshot of a UDP header (using Wireshark), what is the upper (i.e. application) layer protocol encapsulated in this UDP datagram?  e) HTTP f) FTP g) DNS h) TELNET
Answers	c)

Think Template (MCQs)	
Number	3.2
Title	Packet analysis using Wireshark
Type	Fill in the blank
Question	A display filter set to _____, is used to display only DNS packets.
Answers	udp.port == 53 || tcp.port == 53

Think Template (MCQs)	
Number	3.3
Title	Packet analysis using Wireshark
Type	Fill in the blank
Question	A capture filter set to _____, is used to capture ftp traffic to/from host 192.168.1.1
Answers	host 192.168.1.1 and port ftp

Think Template (MCQs)	
Number	3.4
Title	Network-based Evidence Sources
Type	Fill in the blank
Question	A display filter set to _____, is used to display all traffic except ARP, ICMP and DNS packets.
Answers	!(arp or icmp or dns)

Think Template (MCQs)	
Number	3.5
Title	Traffic Analysis challenges
Type	Choose the correct answer
Question	Some of the challenges of traffic analysis are: e) Encrypted traffic f) Large volume of traffic g) Data hiding techniques h) Undocumented protocols
Answers	All of the above.

Extra Template	
Number	3.1
Title	Network Forensics Book
Topic	6. Network Traffic Analysis 7. Protocols Analysis 8. Packet Analysis 9. Flow Analysis 10. traffic analysis challenges
Type	Network Forensics : Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012, ISBN:0-13-256471-8. Section: 4.1 Protocol Analysis

Extra Template	
Number	3.2
Title	On Teaching TCP/IP Protocol Analysis to Computer Forensics Examiners
Topic	3.1. Network Traffic Analysis 3.2. Protocol Analysis 3.3. Packet Analysis
Type	https://www.garykessler.net/library/Protocol_Analysis.pdf Sections: 1. Introduction 2. Protocol Analyzers

Extra Template	
Number	3.3
Title	Wireshark User's Guide
Topic	3.2. Protocol Analysis 3.3. Packet Analysis 3.4. Flow Analysis
Type	https://www.wireshark.org/docs/wsug_html_chunked/index.html Section: 3. User Interface

Extra Template	
Number	3.4
Title	Wireshark display filter reference
Topic	3.2. Protocols Analysis 3.3. Packet Analysis 3.4. Flow Analysis
Type	https://www.wireshark.org/docs/dfref/ section: Display Filter Reference

Extra Template	
Number	3.5
Title	Security Laboratory: Methods of Attack Series
Topic	3.2. Packet Analysis
Type	https://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis. Section: 1. Traffic Analysis

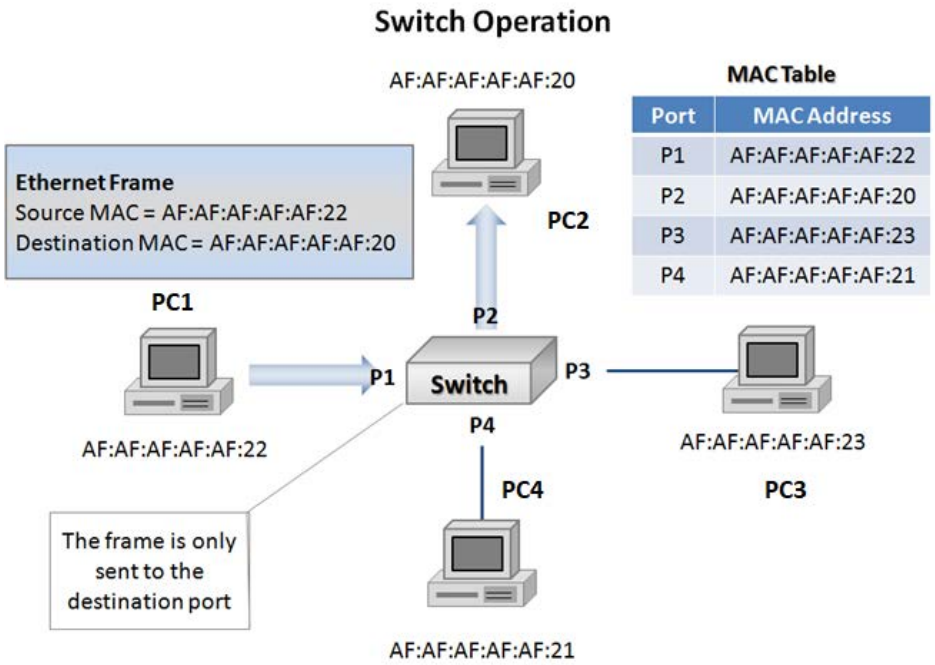
Extra Template	
Number	3.6
Title	Practical Packet Analysis
Topic	3.2. Protocol Analysis 3.3. Packet Analysis 3.4. Flow Analysis
Type	Practical packet analysis: Using Wireshark to solve real-world network problems, 3rd Edition. Sanders, Chris. No Starch Press, 2017. Section: Packet Analysis And Network Basics

Extra Template	
Number	3.7
Title	SynFlood Sample
Topic	3.2. Packet Analysis
Type	https://www.cloudshark.org/captures/ba85949942a0 File: SynFlood Sample.pcap

Extra Template	
Number	3.8
Title	Sample Captures - The Wireshark Wiki
Topic	3.2. Protocol Analysis 3.3. Packet Analysis 3.4. Flow Analysis
Type	https://wiki.wireshark.org/SampleCaptures https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=Http.cap https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=NTP_sync.pcap File: Http.cap File: NTP_sync.pcap

4. Network Systems Forensics

Scope Template	
Number	4
Title	Network Systems Forensics
Introduction	In this chapter, the first section introduces the reader to the main network devices. The second section describes the investigation steps that must be taken for forensics analysis on network devices. The last section addresses the concept of logging, log analysis, and event correlation.
Outcomes	On completion of this chapter the student will be able to: • Design, implement and configure main network systems such as routers, switches and firewalls. • • Conduct a digital forensics investigation on network systems. • • Utilize log analysis and network monitoring solutions in digital forensics investigation.
Topics	• Network device types. • Forensic network device investigation. • Event logging and analysis.
Study Guide	**Task** — **Time** Preparation (introduction and on-line Planning): 1hr Disk-based content: 4hrs Set textbook content: 3hrs Thinking (on-line discussions, review questions) 3hrs Tutorials: 10hrs *Related course work: 2hrs **Total** **23 hours**

Content Template	
Section Number	4.1
Section Title	Network Device Types
Introduction	In this section, we will introduce the main network devices and describe their roles in the network before going into their forensics details. On completion of this chapter the student will be able to design, implement and configure main network systems such as routers, switches and firewalls.
Content	4.1.1 Switches Switches are Layer 2/3 devices that connect multiple computers and switches together to form a network. Switches create an efficient network by isolating the traffic on different switch ports so that each switch port is a separate collision domain which is not the case when a network hub device is used where all computers belong to the same collision domain. This improves performance by reducing the size of the collision domain to the number of PCs connected on the same port. If we have a network operating in a fully switched environment, there will be zero collisions. Figure 4.1 depicts the general switch operation and how this isolation is implemented.  Figure 4.1 Switch Operation

If PC1 sends a frame to PC2, the switch will receive it at port P1 and forwards the received frame to port P2 according to the MAC table of the switch. The switch learns the MAC table automatically.

Types of Switches

1) Managed Switches

These switches support a rich set of features and allow their users to implement and support different network Topologies including complex network Topologies. This makes them suitable for medium and large sized Corporations. Examples of supported features include CLI, VLANs, 802.1x authentication, ARP-caching, port mirroring, event logging, remote access via Telnet/SSH/Web, and SNMP support.

2) Unmanaged Switches

These switches, in general, are self-configured, plug-and-play type that do not require configuration. This makes them suitable for small size network deployments.

3) SDN switches

These switches belong to a new type of network structure, called Software Defined Network (SND). The switch supports the concept of OpenFlow protocol. In SND, a switch takes its switching decision from an SDN controller device. Also, it is possible that a switch performs several roles such as routing and firewalling.

4.1.2 Routers

Routers are Layer 3 devices that connect multiple networks. Routers usually connect a network to an ISP. Also, routers might be used internally in case of large networks such as medium and large sized networks.

The purpose of the router device is to allow route selection from source to destination based on the IP address of the destination. The router accomplishes this task by using its routing table. The routing table can be built dynamically using dynamic routing protocols such as RIP, OSPF, BGP, etc. Also, the routing table can be defined statically using manually entered routes. Figure 4.2 shows the operations of the router using the routing table.

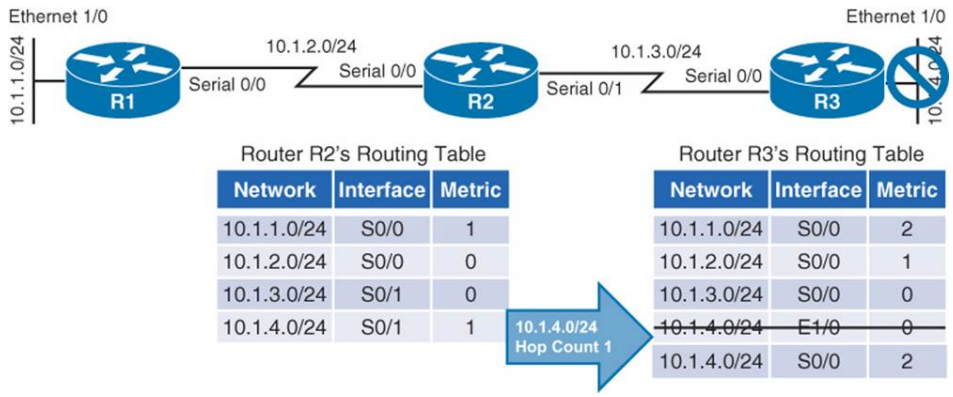


Figure 4.2 Routing Tables

The router consults its routing table for each received packet and routes the packet according to the match between the destination address and its corresponding route in the routing table.

4.1.3 Firewalls

Network firewall devices such as Cisco ASA 5500 model firewalls allow securing the network from potential attacks based on layer 2 to layer 7 properties.

One common security mechanism is the use of Access Control Lists (ACLs). ACLs allow network administrators to permit or deny certain types of traffic according to rules defined based on the IP addresses of the source and/or destination, the type of the protocol, and the port numbers.

The following is an example of how an ACL is defined:

access-list 102 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255

access-list 102 deny ip any any

The list 102 allows traffic from a specific network 10.1.1.X to another specific network 172.16.1.X. The ACL denies all other traffic.

Firewalls also use the concept of stateful packet inspection in which it will inspect all replies to outgoing traffic without compromising the network security by tracking the state of open connections.

In addition, firewalls in general support Virtual Private Network (VPN) capabilities that allow remote secured login to networks. Sometimes, this is done via special VPN devices such as VPN concentrators and VPN clients.

There are two main types of VPNs: Site-to-Site and Remote Access VPN.

Figure 4.3 shows the difference between the two types. A Site-to-Site VPN allows a company to connect securely one network in one location with another network in another far removed location over the Internet. This cuts costs for companies and avoids purchasing expensive dedicated lines over long distances.

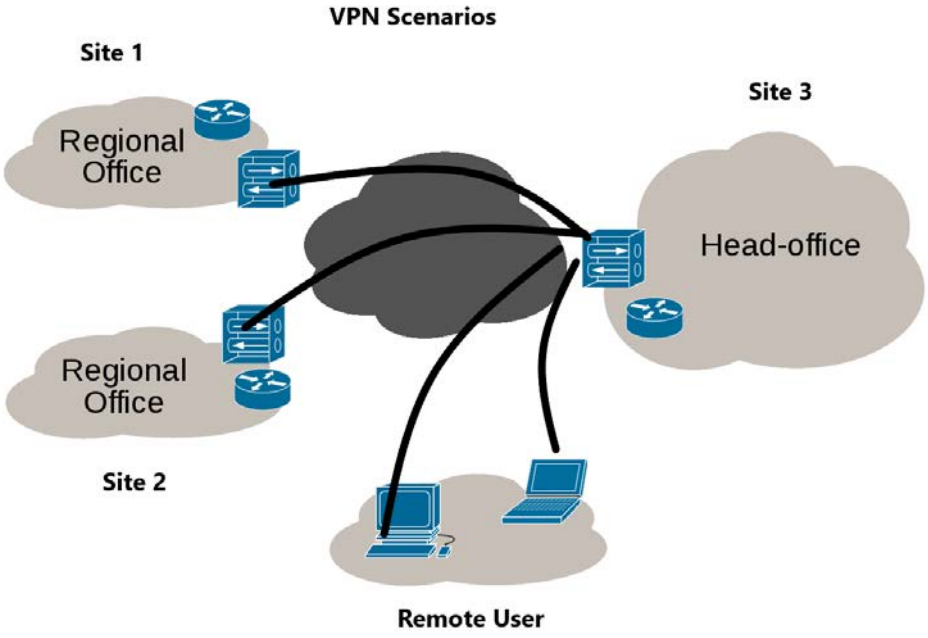


Figure 4.3 VPN Scenarios

In the case of a remote access VPN, it allows users to access a corporate network remotely using their desktops, laptops, and smartphones. On one hand, this makes it convenient for employees and third-party contracted companies to access resources without requiring to be physically within the network. On the other hand, this creates a forensics challenge.

4.1.4 Network Hosts

Network hosts of all types including servers, desktops, laptops, mobile phones, printers, etc., are all important component of the network.

Network servers such as file servers, domain servers, email servers, and DHCP servers provide services to the end users that end up consuming these services using other types of hosts (PCs).

Network hosts, in general, contain important information about user behaviour with respect to the offered service. This can provide some helpful evidence in certain cases.

	4.1.5 Internet of Things (IoT) The use of IoT devices has grown rapidly in the past few years. According to Cisco, 50+ billion IoT devices are expected to be live in 2020. This has necessitated the consideration of these devices in any network analysis. IoT devices are used in smart homes, smart cities, hospitals, and companies. 4.1.6 Web Proxies A web proxy solution has become popular as part of the implementation of large corporate networks. A web proxy allows filtering of certain web requests along with caching common requests for web pages. Caching speeds up the retrieval of web traffic. Web proxies are an important point of investigation as they deal with the largest portion of Internet traffic of any organization. 4.1.7 Mobile Devices Since the invention of smartphones in 2007, mobile devices have evolved to become powerful devices with significant computing resources and numerous software applications and options. Despite the many advantages of smartphones, they represent a new type of threat to networks as they can connect to WiFi network and 3G/4G networks at the same time. Their mobility and compact size make them difficult to discover and manage. 4.1.8 Other Network Devices In addition to the aforementioned network devices, there are many other specific types that are not common but are used in certain networks depending on the deployment options and the size of the network. This includes Intrusion Detection Systems (IDS), Intrusion Protection Systems (IPS), wireless access points, modems, bridges, and gateways.

Content Template	
Section Number	4.2
Section Title	Systems Investigation
Introduction	In this section, we will explore network device forensics options and steps. The section starts with the common actions that must be taken with the network device regardless of its type. Next, specific action steps are mentioned according to the type of network device.

Content	4.2.1 Device Access The first thing that requires investigation when dealing with network devices is to study the type of access they provide and the authentication options in order to access the system. The most common access methods include Telnet, SSH, and Web Access. Telnet and SSH are convenient means for devices that support a command line interface (CLI). The first step in the access process is the authentication option. This can be accomplished via a hardcoded password, a local database, or a shared database using an external solution such as TACACS+ from Cisco and RADIUS. Figuring out the authentication options can help to track who can login to the system. 4.2.2 Configuration The second element that must be reviewed is the configuration of the network device, where it is backed up, the tools/protocols used to achieve that, and the security enabled in the configuration. 4.2.3 Events and Log options One important element to study is the logging options of the device, whether logging is enabled or disabled, and the location of logged events. The log file(s) can be extracted for further analysis. See section 4.3 for more details on this. 4.2.4 Statistics and reports Modern and high-end devices provide detailed statistics about traffic, and device ports or interfaces. This includes the number of packets and frames delivered or failed for each port. In addition, reports of overall system events are usually stored such as last system reboot time and so on. Statistics and reports can provide valuable evidence and an indication for the presence of some issue. Figure 4.4 shows an example of the output of a Cisco router interface. It shows several helpful statistics. Router# **show interfaces** Ethernet 0 is up, line protocol is up Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c) Internet address is 131.108.28.8, subnet mask is 255.255.255.0 MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255 Encapsulation ARPA, loopback not set, keepalive set (10 sec)

ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
1127576 packets input, **447251251** bytes, 0 no buffer
Received **354125** broadcasts, 0 runts, 0 giants, **57186*** throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5332142 packets output, **496316039** bytes, 0 underruns
0 output errors, **432** collisions, 0 interface resets, 0 restarts

Figure 4.4 Router Statistics

4.2.5 SNMP protocol

One important point to be investigated is the use of the SNMP protocol within the network. SNMP allows network administrators to manage their network using SNMP-enabled devices. In the case of SNMP use, SNMP tools can be utilized to provide valuable network information for the network overall.

4.2.6 Switch Considerations

For networks that involve switches, several issues must be considered during the investigation. Examples of such issues include the use of VLANs, port security, CAM memory, and port mirroring.

Virtual Local Area networks (VLANs) are used to create logical groups within switched networks where PCs that are connected to the same switched network can be isolated for security and performance reasons.

Figure 4.5 shows an example of how VLANs used. Three groups of hosts (Accounting, Engineering, and VOIP) have been isolated using VLANs where no host from one group can reach another host from another group directly.

It is like creating a physical isolation.

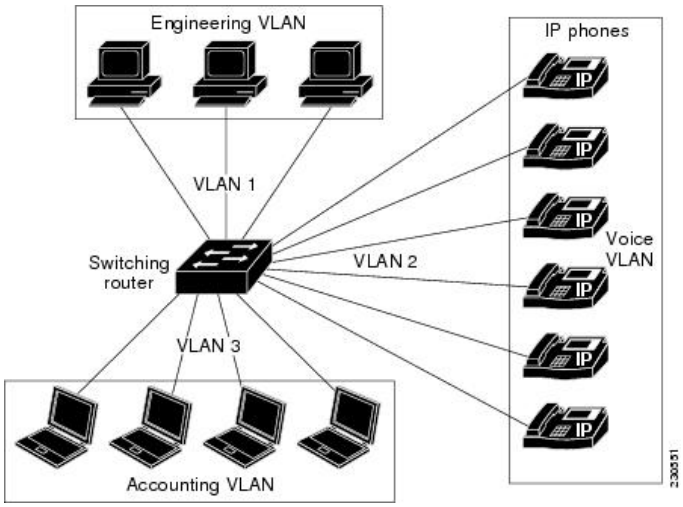


Figure 4.5 VLAN Example

Switches support port security as well. Port security allows a switch to restrict the hosts that can access the network by associating the MAC address to the port.

The switch CAM memory is an area that is used to track the active hosts and their MAC addresses. Although this is a volatile memory, it can provide the investigator with important artifices if collected.

Port mirroring allows a network administrator to mirror all the switch traffic to that port. Any host connected to a mirrored port will be able to see the entire traffic that passes through the switch. This is a helpful feature for analysing the traffic of the network.

4.2.7 Router Considerations

In addition to studying the overall statistics generated from a router device, the router table provides important information about the paths followed by the network traffic.

The interfaces and the connections of the routers help figure out the network topology.

4.2.8 Access Point Considerations

Wireless networks suffer additional security issues due to the openness of the communication where anyone could attempt to join the network without a physical connection.

Access points represent the hub of wireless networks when wireless infrastructure mode is deployed.

	Wireless networks use several authentication options and protocols. Protocols such as WEP, WPA, and WPA+ are used for security authentication and encryption. One of the main issues to be investigated is the presence of malicious association. In this situation, a wireless device is configured to appear as a legitimate access point, allowing the hackers to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point. This is known as man in the middle attack where that intermediate wireless device sits in between the user and the real network and intercepts everything done by the user. All access points must be reviewed. Also, the range of the wireless networks must be studied as coverage that goes beyond the needed zone might grant outsiders access to the network. 4.2.8 Mobile devices considerations physical control over mobile devices is difficult to achieve in an enterprise due to their small size and mobile nature. They introduce many threats, they use untrusted applications, untrusted contents, and connect to untrusted networks.

Content Template	
Section Number	4.3
Section Title	Event Logging and Analysis
Introduction	In this section, we discuss the concept of logging, its importance, how to analyse log files and correlate the results from several events and log sources. On completion of this chapter the student will be able to utilize several log analysis solutions in digital forensics investigation.
Content	4.3.1 Introduction network devices generate event logs. Event logs are records that provide information about the state of the system and/or the environment at a given time. Diverse systems produce an array of event logs. Event logs may incorporate data about a system (for example, server logins and logouts), start-up and shutdown times, performance issues, or simply routine information, for example, the server farm temperature. Event logs might be sent from individual devices to a local server, or sent to various servers There is a vast number of event log designs and formats, which represents a challenge for their analysis. Event logs are considered important for the following reasons: • event logs contain information directly related to network functions. • event logs include records of network activity, such as remote login histories. • event logs have been transmitted over the network and therefore created network activity. 4.3.2 Log generators The sources of event logs include the following • Events generated from operating systems such as Windows, Linux, or UNIX-based operating systems • Application and server events such as web, database, and DNS servers

• Network device events, such as switch events

• Other physical devices events, UPS events

Figure 4.6 shows an example of a windows sever event log (Event Viewer application).

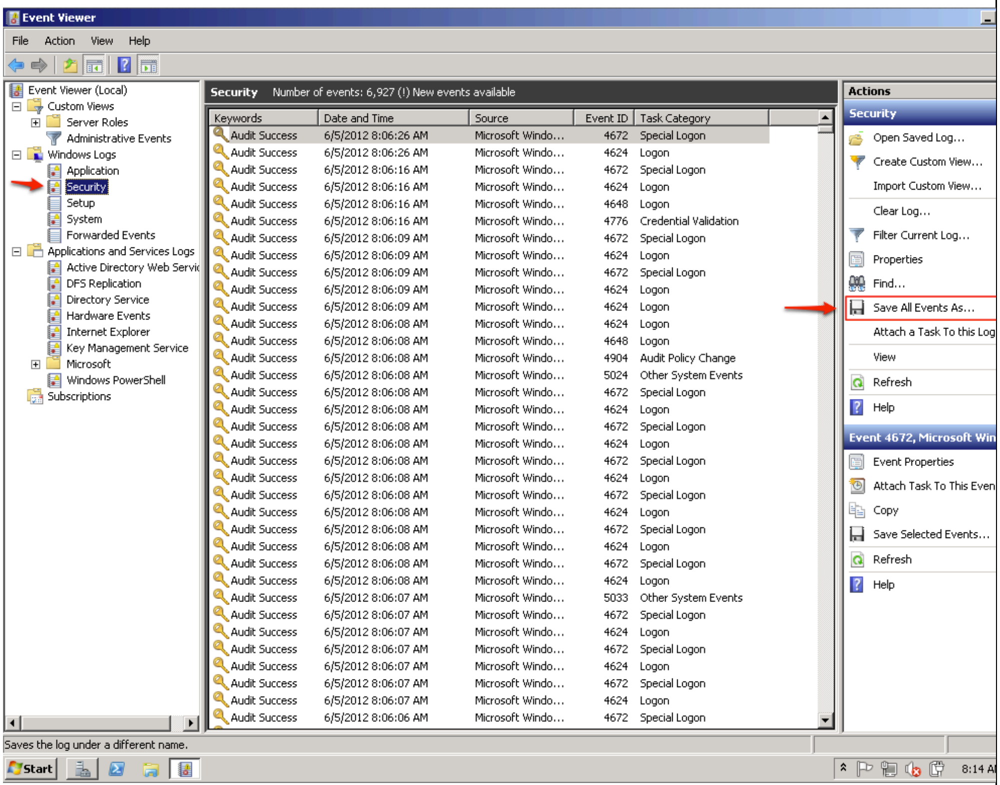


Figure 4.6 Events Viewer in Windows system

Note how a Windows system categorizes the events into five different categories:

- Application
- Setup
- System
- Security
- Forwarded events

In a Linux system, Syslog is used to track system logged events.

Figure 4.7 shows a Linux example.

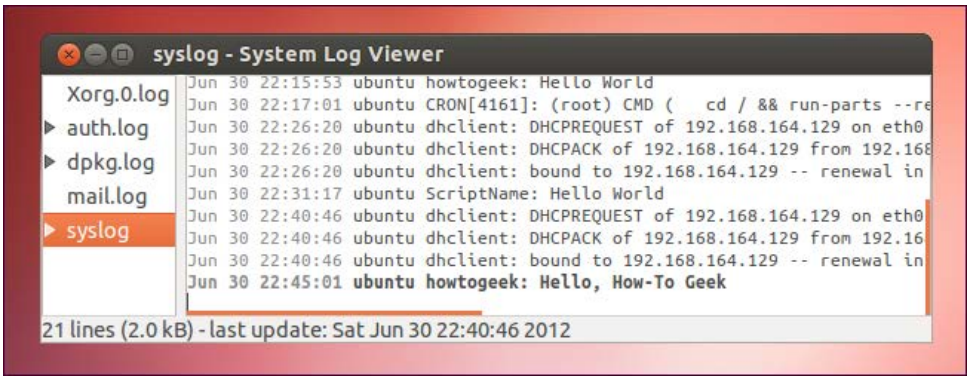


Figure 4.7 Events using System Log Viewer in Linux

Cisco devices also support logging . Figure 4.8 shows a sample.

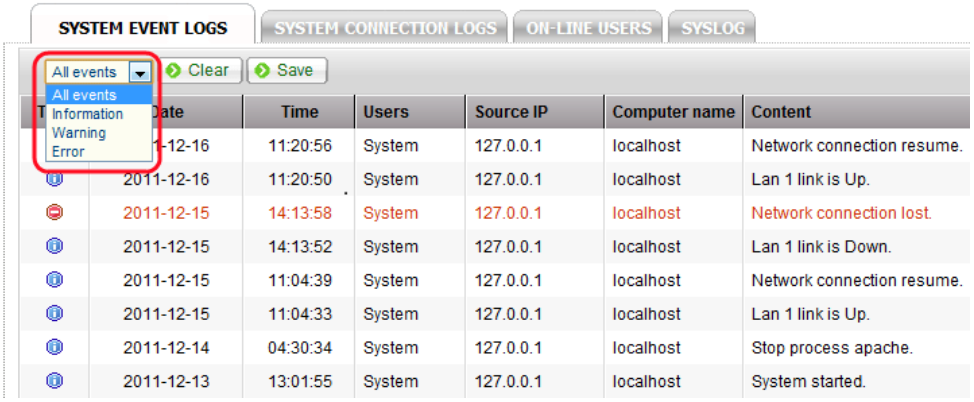


Figure 4.8 Events logging in Cisco devices

4.3.3 Logging Architectures

Events can be logged in three different ways:

- Locally

Logs are gathered on local hard drives. This is the default setup for most working systems, applications, physical gadgets, and system hardware. Local log accumulation presents issues for investigators.

- Remote decentralized

Logs are sent to various remote locations throughout the network . Specific logs might be stored on various servers. This is usually the approach in situations where there is decentralized administration of IT assets, for example, in colleges where singular divisions or labs deal with their specific local servers.

- Centralized

	Logs from many sources are centralized in one location. This represents the best option for a forensics analysis task for the following reasons: • Remote servers, where logs are stored, are more protected from unauthorized modifications. • Timestamps are automatically unified in this case. • Centralized management typically allows for easy access to log data. • One source can be easily exposed to an analysis tool. 4.3.4 Analyzing log events Reading the log of events and learning about the network from it is a useful task for investigating the status of the network and for performing some forensics tasks. Manual reading and analysis become a challenge when dealing with a large number of events. There are software applications and tools that are specialized in analyzing log events and correlating among these events. An example of such tools is Splunk. In general, we use one or more of the following to analyze the log. • Filtering: selecting logs based on certain helpful criteria such as time or the address of the sender/recipient. • Activity Patterns: Look for patterns of activity and suspicious behaviours • Fingerprinting: correlating events and complex patterns. Figure 4.9 shows Splunk tool for log analysis.

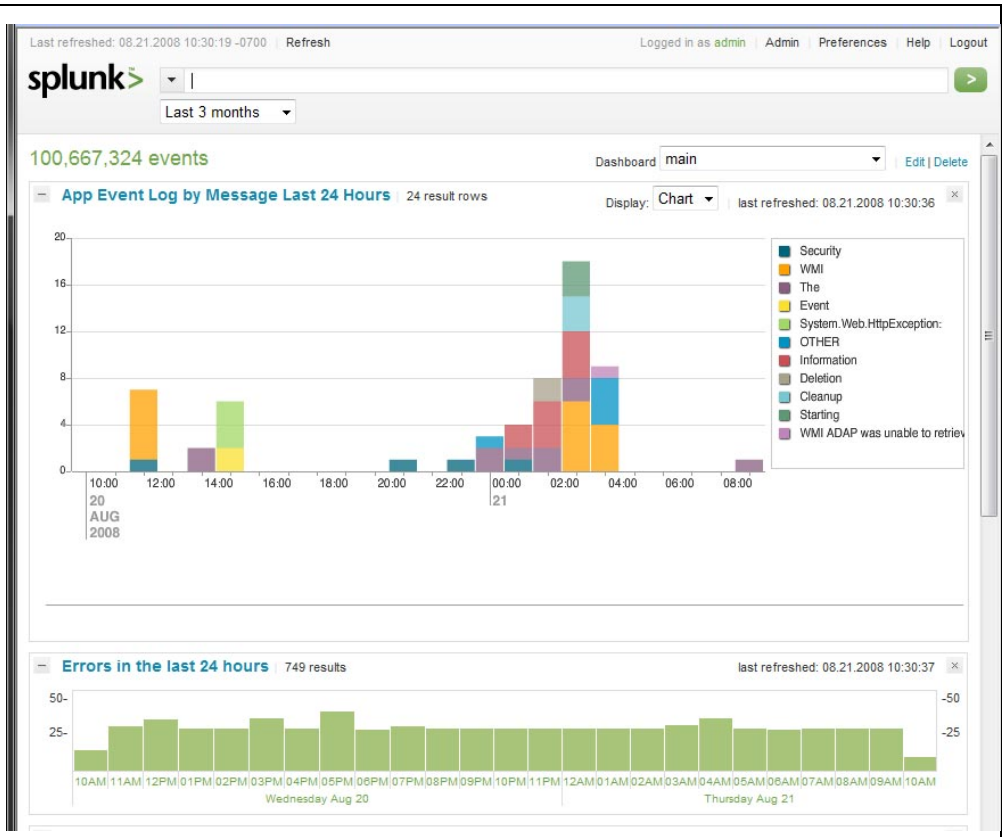
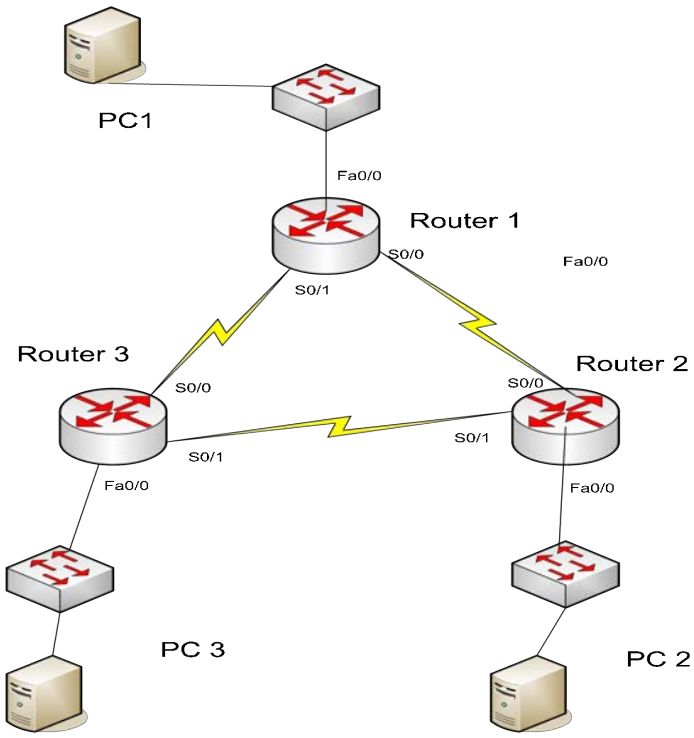


Figure 4.9 Splunk for log Analysis

Activity Template	
Number	4.1
Title	Industry switches and routers
Type	Review
Aim	To familiarize the student with the main types of industry switches and routers compare among them. Developing students' critical thinking abilities as well as research and comparison skills.
Description	Study market switch and router products. List top 3 companies that provide such products. Compare the main features offered for the switches. Repeat the comparison for routers too.
Timeline	2 hours
Assessment	List the main companies and their products 40%. Routers comparison 30%. Switches comparison 30%.

Activity Template	
Number	4.2
Title	Switches and Routers Configuration
Type	• Research • Review
Aim	To familiarize the student with the main steps involved in configuring networking systems such as routers and switches Develop the student's technical skills in building and configuring modern computer network using industrial simulators.
Description	The student will be given a networking scenario requiring configuration. The network includes routers, switches, and some PCs. The activity should be completed on a real network or using a simulator such as Cisco Packet Tracer. Build the following scenario  Using packet tracer software, create and configure the given network with the following settings: Passwords, for all network devices, set the password as 'class' for each. Router 1: router name is Router1 Fa0/0 192.168.1.1 with mask /24 S0/0 192.168.4.1 with mask /24 S0/1 192.168.5.1 with mask /24 Router 2: router name is Router2 Fa0/0 192.168.2.1 with mask /24

	S0/0 192.168.4.2 with mask /24 S0/1 192.168.6.1 with mask /24 Router 3: router name is Router3 Fa0/0 192.168.3.1 with mask /24 S0/0 192.168.5.2 with mask /24 S0/1 192.168.6.2 with mask /24 Set the PCs address as the following: PC 1: IP address is 192.168.1.10 with mask /24 and default gateway: 192.168.1.1 PC 2: IP address is 192.168.2.8 with mask /24 and default gateway: 192.168.2.1 PC 3: left as a student exercise: pick an IP address, subnet-mask, and default gateway that can work with this network design. Routing: Use static or dynamic routing so all PCs can ping each other.
Timeline	5 hours
Assessment	Based on completion rate 100% means complete and functioning network

Activity Template	
Number	4.3
Title	Windows Event Viewer
Type	• Research • Review
Aim	Upon completion of this activity the student will be able extract security events of interest from the windows event viewer and describe each event type.
Description	How to use windows event viewer. 1) Access the Windows event viewer depending on your windows version. 2) Create one screen shot for each event category (application, system, etc.) 3) Answer the following questions: a) What is the difference between the following types of events? Error, Warning, Information, Success Audit, and Failure Audit. b) What does each category track? (System, application, security, etc.)
Timeline	2 hours
Assessment	Steps followed and providing screen shots 50%. Answering questions 50%.

Activity Template	
Number	4.4
Title	Linux Logging
Type	• Research • Review
Aim	Upon completion of this activity the student will be able to extract events of interest from the standard Linux log files.
Description	Access a Linux system (or virtual box with Linux installed). Perform the following steps and provide screenshots: 1) Enable syslog locally. 2) Send a log message to another machine (or from other machine). 3) Make the remote logging secure. 4) View the /var/log directory and explain the contents of two of its files. Provide screen shots for each step.
Timeline	2 hours
Assessment	Each step 4 x 25%

Activity Template	
Number	4.5
Title	Packet Tracing
Type	• Research • Review
Aim	Become familiar with a packet sniffer Develop the student's technical skills in monitoring and analyzing network traffic in order to extract digital forensic artifacts.
Description	1) Install Wireshark software. 2) Start the software and the sniffing process. 3) Run an application that generates network traffic. 4) Capture network traffic. 5) Analyze the traffic and show the IP address, mac address used and ports. Show screenshots of your results.
Timeline	2 hours
Assessment	Each step 5 x 20%

Activity Template	
Number	4.6
Title	Using Splunk Software
Type	• Research • Review
Aim	Become familiar with Splunk software Develop the student's technical skills in collecting and analyzing different types of logs in order to extract digital forensic artifacts.
Description	1) Install Splunk software. 2) Start the software. 3) The instructor will provide you with several log files. 4) Load the log files and analyze them. Show screenshots of your results.
Timeline	2 hours
Assessment	Each step 4 x 25%.

Think Template (MCQs)	
Number	4.1
Title	Network Systems Types
Type	Choose the correct answer
Question	Which of the following network devices functions mainly at layer 2 and isolates collision domains
Answers	A. Router **B. Switch** C. Firewall D. Web proxy

Think Template (MCQs)	
Number	4.2
Title	Network Device Types
Type	Choose the correct answer
Question	Which of the following network devices finds the path from source to destination
Answers	**A. Router** B. Switch C. Firewall D. Web proxy

Think Template (MCQs)	
Number	4.3
Title	Network Device Types
Type	Choose the correct answer
Question	Which of the following network devices can be used to cache web requests and optimize web browsing?
Answers	A. Router B. Switch C. Firewall **D. Web proxy**

Think Template (MCQs)	
Number	4.4
Title	Network Device Types
Type	Choose the correct answer
Question	A switch functions using
Answers	A. IP address **B. MAC address** C. TCP/UDP Port number D. User ID

Think Template (MCQs)	
Number	4.5
Title	Network Device Types
Type	Choose the correct answer
Question	The following allows connecting two networks securely
Answers	A. Router B. Switch C. BYOD **D. VPN**

Think Template (MCQs)	
Number	4.6
Title	Systems Investigation
Type	Choose the correct answer
Question	One of the followings allows a switch to isolate one group of PCs from others
Answers	**A. VLAN** B. CAM C. Port Security D. VPN

Think Template (MCQs)	
Number	4.7
Title	Event Logging and Analysis
Type	Choose the correct answer
Question	Which of the following tools can help analyze logs
Answers	A. Wireshark B. Packet tracer **C. Splunk** D. Cisco IOS

Extra Template	
Number	4.1
Title	Network Forensics: Tracking Hackers through Cyberspace by Sherri Davidoff and Jonathan Ham.
Topic	• 4.1 • 4.2 • 4.3
Type	Network Forensics: Tracking Hackers Through Cyberspace, Sherri Davidoff, Jonathan Ham, Prentice Hall, 2012. ISBN-10: 9780132564717 ISBN-13: 978-0132564717

Extra Template	
Number	4.2
Title	Applied Network Security Monitoring: Collection, Detection, and Analysis.
Topic	• 4.1 • 4.2 • 4.3
Type	Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress; 1 edition (December 19, 2013). eBook ISBN: 9780124172166 Paperback ISBN: 9780124172081

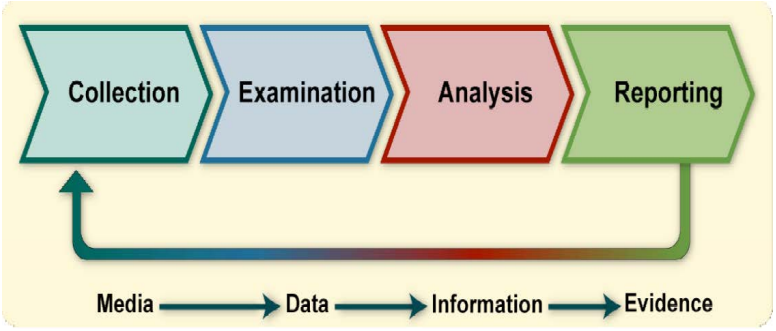
Extra Template	
Number	4.3
Title	Practical Packet Analysis, 3rd Edition Using Wireshark to Solve Real-World Network Problems by Chris Sanders.
Topic	• 4.1 • 4.2 • 4.3
Type	Practical Packet Analysis, 3rd Edition Using Wireshark to Solve Real-World Network Problems by Chris Sanders. Book/Chapter (ISBN) ISBN-13: 978-1-59327-802-1

Extra Template	
Number	4.4
Title	Splunk Software
Topic	• 4.3
Type	URL: https://www.splunk.com/

Extra Template	
Number	4.5
Title	Packet Tracer Software
Topic	• 4.1 • 4.2
Type	URL: https://www.netacad.com/courses/packet-tracer

5. Network Evidence Collection and Analysis

Scope Template	
Number	5
Title	Network Evidence Collection and Analysis
Introduction	In this chapter, the process of collecting network evidence from all available sources is described. Large volumes of log entries and other information must be aggregated, normalized, stored and managed by a log manager. After the collection step, follows examination and analysis of the output of collection step. Various techniques and technologies are used across multiple categories of tools. Among these: AI, Machine Learning, Statistical and Behavioural Analysis and others. tools that assist and automate the analysis of the voluminous data are investigated by means of practical example. Such analysis would be impossible for any investigator without the help of such tools.
Outcomes	1. On successful completion of this chapter, the student should be able to describe how network evidence is collected, and be able to use tools to normalize, aggregate and store that evidence. 2. The student will be able to apply best practice for the management of network evidence and logs after collection. 3. The student should be able to understand and apply the various scientific and computational methods used to process network evidence and reach conclusions.
Topics	5. Introduction 5.1. Network Evidence Collection 5.1.1. Identifying sources of evidence 5.1.2. Evidence Handling 5.2.1 Log Managers 5.2.2 Log Managers Examples 5.3.1 Security Incident and Event Management (SIEM) 5.3.2 SIEM Tools 5.3.3 SIEM Technologies 5.4 Reporting
Study Guide	– Required time: 18 hours • Required hardware/software. – Sys-log-ng, AlienVault SEIM, linux – Linux Workstation or virtual machine • Required external resources including links and books. – NIST Special Publication 800-86 – NIST SP 800-101 Rev. 1 – NIST SP 800-72 – Reference Book Samir Datt, "Learning Network Forensics, 2016 – SP 800-92: Guide to Computer Security Log Management, https://csrc.nist.gov/publications/detail/sp/800-92/final – https://www.syslog-ng.com/products/open-source-log-management/ – https://www.splunk.com/ – https://www.ibm.com/us-en/marketplace/ibm-qradar-siem, https://www8.hp.com/us/en/software-solutions/integrated-security-solutions-arcsight/index.html

Content Template	
Section Number	5
Section Title	Introduction
Introduction	In this chapter, we revise the basic phases of the forensics process, which include the following four phases: collection, examination, analysis and reporting.
Content	The National Institute of Standards and Technology (NIST) provides a timeline for forensics: • Collection: During this phase, the data associated with a specific kind of event is identified, collected, and stored securely. The collected data is the digital evidence, which has to be properly, collected, maintained, transferred according to best practices in the industry and adhering to the legal system of the country. This phase also includes interviewing witnesses and interviewing suspects with the help of any gathered evidence.. • Examination: The next step is the examination of the evidence using appropriate, accredited and certified tools to analyze the collected evidence . The major task in this phase is to search for and identify any potential evidence related to the incident. The analysis carried out in this phase is executed on an image of the evidence, not the original copy, in order to preserve the integrity of the original . Multiple techniques can be used to generate such copies depending on available tools and operating environments. • Analysis: In this phase, we analyze what has been gathered in the previous phase using tools and techniques that can convert available information into a solid evidence that helps answer the "W questions: what, when, where, why, how?". In this phase, we develop a complete understanding of the case and possible motives behind it. It might be possible to explicitly determine the type of the case: accidental, disgruntled employee, industrial espionage, etc. • Reporting: The findings of our investigation should be presented to the owner of the case; management or court, in a professional and acceptable format. The report should contain clear facts and evidence, not opinions, regarding the findings. It should describe and document the forensics process followed including tools and techniques applied. Sometimes, the report may contain recommendations to prevent such incidents in the future, especially if it was the result of a vulnerability exploitation or policy violation .  Figure 5.1: Forensic Process (Timeline) [1]

	Reference: NIST Special Publication 800-86, NIST SP 800-101 Rev. 1, NIST SP 800-72 • URL:https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

Content Template	
Section Number	5.1
Section Title	Network Evidence Collection
Introduction	In this section, we will learn how to identify the different types and sources of evidence and how to properly collect evidence .
Content	Evidence obtained from Media Analysis. This can include the following sources: 1. Memory of the individual computers under investigation 2. Hard drivers, CDs, DVDs, SSDs, USB devices, and backups 3. Internal, external network or cloud During the digital forensic process, an investigator should analyze any evidence residing on any of the above mentioned sources. Memory analysis might uncover evidence of programs running and temporary data that would otherwise be lost when the computer is powered down. Evidence collection also includes all other types of media such as: hard drives, SSDs , CDs, DVDs, etc. The investigator should also review all available backups; this action is needed when data is deleted from a computer. The investigator is responsible for the integrity of the evidence media. The media has to be removed carefully, sealed, padded with special material and properly protected while transported to the forensics lab. The investigation must be carried out on an evidence image, which is made using special tools and write-blockers, while keeping the original evidence media intact. In a network, evidence can come from sources like: 1. Routers, Intrusion Detection software and Firewall logs 2. Sniffers of traffic 3. Internet Service Providers (ISP)

Content Template	
Section Number	5.1.1
Section Title	Identifying sources of evidence
Introduction	In this section, we identify sources of logs and evidence that we use in our forensic investigation.
Content	• Evidence from logs: A log is a record that stores all the activities and information passing through a device or through outside agents on a device. logs are an important part of the forensic process, where the examiners can examine data logged on a network router, firewalls, intrusion prevention and detection systems, antivirus servers, etc. Also there are other logs including operating system event logs, application logs, and so on. Logs are very important and can provide very useful information to the investigation, especially if the incident takes place in a network. In addition, these logs are a detailed record of access to various Internet resources that are provided by the ISP. This can include details related to log on/ log off events, user names, resources accessed, online content, online activity, IP addresses, date and time of usage, and the duration of use. The investigator reviews log data to identify any evidence of incoming/outgoing traffic that can be linked to the suspect abnormal behavior. If the case involves data leakage then the investigator might need to examine the ISP records, which requires cooperation and approval . • Evidence obtained through software analysis: This can include the following sources: AntiVirus, email, files, timestamps, metadata, webservers, browser software logs. The investigator looks for evidence in systems and tools installed on a computer/server or a network to provide operational and security services such as: anti-virus, email, file servers, log managers , etc. and looks for timestamps and metadata that can be very helpful establishing evidence of a crime or violation of a security policy. Examining such systems might answer question like who created, edited or deleted a file such as a word document that contains critical information. Web servers and browsers can provide important information about a user's activity and history and as such provide evidence that helps with a forensic investigation.
	Reference: Book Samir Datt, "Learning Network Forensics, 2016

Content Template	
Section Number	5.1.2
Section Title	Evidence Handling
Introduction	In this section, we will learn what is digital evidence and how to handle it.
Content	In the real world, evidence is material presented to the court to prove the validity of a hypothesis or its invalidity. In order for evidence to be presentable to the court, it has to be authentic, accurate, complete, convincing and admissible. Once the sources of evidence are identified, the next critical aspect is how to handle it. There are some widely-agreed upon rules to handle evidence. 1. Handle the evidence with care The evidence has to be handled with care. The goal is to reduce any damaging effects to the evidence. When it is essential for the investigator to interact with the evidence, it must be done in a manner that is least intrusive and completely documented. 2. Always work on an image As with all forensic investigations, any interaction with the original evidence in digital form might compromise it . Therefore, the investigator should create copies before performing any processing or log file analysis because the metadata of files might change as a result of the analysis If the original files are unaltered, the investigator can prove more easily that they are authentic and in their original form. When using a log file asevidence in court, an investigator is required to present the original files in their original form. It is a best-practice to create a forensic copy of the digital evidence and ensure its authenticity then carry out further investigations 3. Documentation In an investigation, evidence is only as good as the process followed to obtain it. Unless proper processes with the correct precautions are followed, the process of acquiring and authenticating the evidence may be flawed unless we have a clear-cut documentation attesting to the fact. Therefore, rigorous documentation across the entire evidence lifecycle is essential . Chain of Custody (CoC) is the documentation of all the actions taken during an investigation using the evidence and all information about it including ownership, transportation, storage, etc. and it's a necessity in solving the case. The evidence's chain of custody is very important to the investigation and the case. evidence might be refused by the court if not maintained properly. the chain of custody includes documentation detailing who obtained the evidence and secured it, where was the evidence found, when it was obtained, who had control or possession of the evidence, where the evidence was stored? (secure storage in a monitored vault is common). The integrity of the evidence should be maintained from the time it is collected until the time it is presented to court. So, to maintain the chain of custody, the investigator must make sure the evidence has not been altered or modified using reliable hashing algorithms and digital signatures.

	The evidence should be stored in a vault, which is continuously monitored by an alarm system or video surveillance system or both. In addition, the physical space in which the evidence resides must be protected by electronic physical access control systems. Also, when an investigator or a network administrator moves the evidence such as log files from a server, and after that to an offline device, the investigator should keep track of the locations where the log files went and what other devices they passed through. The investigators can use technical or nontechnical methods, such as CRC, MD5 , SHA and other authentication and hashing tools to maintain chain of custody.
	Reference: Book - Samir Datt, "Learning Network Forensics, 2016

Content Template	
Section Number	5.2
Section Title	Network Evidence Analysis
Introduction	In this section, we discuss network evidence analysis, which comes after the collection of evidence. The result of this activity is information and conclusions about any breaches or attacks.
Content	After the collection, normalization and aggregation of every available network log as discussed in section 5.1, a new phase of the forensic life cycle begins, which is the analysis phase. All available sources of network information should be gathered and correlated so that useful information can be extracted about the breach. In this section we introduce all components that play a role in this analysis and investigation.

Content Template	
Section Number	5.2.1
Section Title	Log Managers
Introduction	In this section, we introduce log managers, which are the first components consulted in an analysis .
Content	Log managers are central repositories and tools that store network evidence (logs) from any possible source in the network. The sources of logs include: network devices, servers, operating systems, intrusion detection systems, firewalls, anti-virus systems and any other possible source. All these kinds of logs are collected and aggregated in a centralized database, which is responsible for and should be capable of housing Giga-Bytes of data for a reasonable period of time. Because of the large volume of logs entries generated every second, it might be sometimes impossible to keep every log because of limited storage resources availability and the negative impact on performance. So, in some cases, only selected logs are stored and analyzed. In other cases, a lifetime is enforced on the logs, so the logs should at least stay in the log manager for a specified period of time that is usually enforced or recommended by some standard or accreditation institution. In many cases, we find institutions maintain logs for at least 180 days (6 months) to satisfy law enforcement requirements or best practices . It is very useful for any investigation to retrieve such logs covering the longest time period possible, especially with the advanced hiding techniques used by sophisticated attacks that might remain undiscovered for months or even years. Because of the large volume of log entries generated every second from hundreds of devices, any entity collecting logs would typically implement SAN storage to accommodate such valuable data. Reference: SP 800-92: Guide to Computer Security Log Management, URL: https://csrc.nist.gov/publications/detail/sp/800-92/final

Content Template	
Section Number	5.2.2
Section Title	Log Manager Examples
Introduction	In this section, we introduce examples of log managers.
Content	Many solutions and products are available to accommodate large logs emanating from various sources, which will be part of the forensic evidence trail . 1. Syslog-ng: Syslog-ng is a free and open-source tool implementing the syslog protocol for various operating systems. It is used to collect logs from any source, parse, classify, rewrite and correlate logs from across the network infrastructure and store or route them to log analysis tools.

It has filtering capabilities, flexible configuration options and adds important features to syslog, like using TCP for transport.

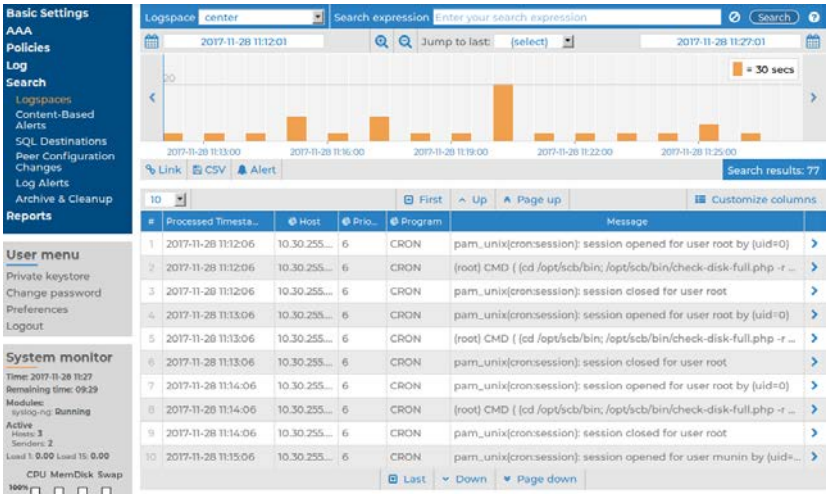
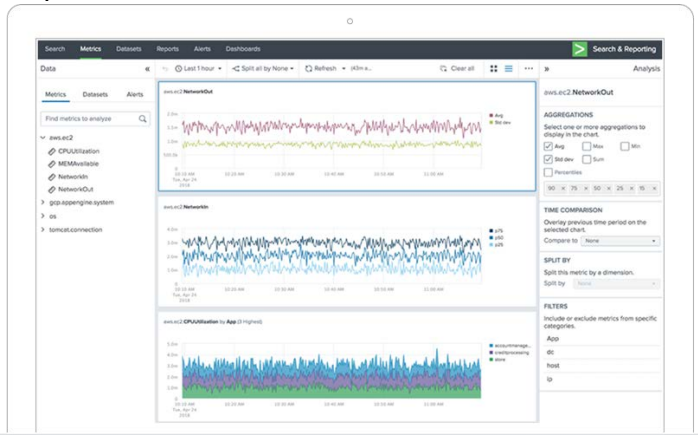


Figure 5.2: SysLog-ng screen shot

2. Splunk:
   Splunk was originally a log manager that captures and correlates logs in a repository to uncover attacks . It can generate alerts and reports and display information in dashboards.
   An enterprise version of Splunk exists, which falls under a new category of security products discussed in the next section.

References:
https://www.syslog-ng.com/products/open-source-log-management/
https://www.splunk.com/

Content Template	
Section Number	5.3.1
Section Title	Security Incident and Event Management (SIEM)
Introduction	In this section, we introduce a more advanced category of tools for working with logs .
Content	Security Incident and Event Management (SIEM) is a new category of security management tools that started to dominate the security and forensics industry. Such tools combine Security Information Management and Security Event Management (logs). A SIEM product can have its own log repository or connect to any available log managers/servers, in addition to connecting directly to any source of logs/events/evidence. We will explore some of these technologies in the next sections.

Content Template	
Section Number	5.3.2
Section Title	Security Incident and Event Management (SIEM) Tools
Introduction	In this section, we introduce a more advanced category of tools for working with logs
Content	1. HP ArcSight ArcSight is one of the most powerful SIEM tools in the market owned by HP. It provides comprehensive connecters with almost all network log sources, visibility of all network activity, compliance to security standards like, ISO, FISMA, SOX, PCI-DSS, HIPAA, etc. It employs behaviour based anomaly detection to report any deviations from the usual network behaviour. 2. Splunk Splunk Enterprise is a completely different category of products that differs from the original Splunk product. It is a SIEM tool with many features including filtering, correlation, analysis and presents conclusions to operators. It can collect data from any source. It implements artificial intelligence and machine learning methodologies to provide SIEM functionality.  Figure 5.3: real time Splunk analysis 3. IBM QRadar QRadar is IBM's SIEM solution. It provides SIEM services by consolidating logs from applications, hosts, devices, networks and endpoints. It correlates items across all logs and aggregates related events into single alerts to accelerate incident analysis and remediation. QRadar SIEM can be installed inside the enterprise network or can be implemented as a cloud-based service. 4. AlienVault AlienVault is an open-source SIEM tool, but with limited features. The full-featured is commercial. It is a good option for institutions with a limited budget. References: https://www.splunk.com/, www.alienvault.com/, https://www.ibm.com/us-en/marketplace/ibm-qradar-siem, https://www8.hp.com/us/en/software-solutions/integrated-security-solutions-arcsight/index.html

Content Template	
Section Number	5.3.3
Section Title	Security Incident and Event Management (SIEM) Technologies
Introduction	In this section, we introduce some of the technologies used by SIEM tools .
Content	1. Artificial Intelligence (AI). Artificial intelligence is an area of computer science where machines analyse the environment and available information to deduce facts and take decisions. The new trend in security and forensics tools is to rely heavily on automated AI systems, especially given the large volumes of data involved, where it is impossible for any human to be capable of processing without machine help. 2. Machine learning Machine learning technologies can be used to analyze SIEM logs using algorithms that build mathematical models based on training data samples, in order to find relationships, make correlations, do predictions, give recommendations or make decisions without being explicitly programmed to perform the task [1]. Machine learning is used in the detection of network intrusions and is able to provide evidence of such intrusions. 3. Statistical Analysis Network traffic is monitored to detect any statistical anomalies in the use of network resources by any actor or user. Based on this, SEIM tools might take decisions to block connections or raise alarms. An event such as a large data transfer from one folder to another might trigger an alarm to security administrators and the details of this transfer might serve as evidence. 4. Behaviour Analysis Network subjects and objects are monitored and their behaviour is modeled , so if any deviation from normal behavior is detected an alarm is sent to the security administrator. Events like logins outside regular work hours is an example of behaviour that should be monitored to enforce an access control policy and to establish evidence if needed. References: [1] Bishop, C. M. (2006), Pattern Recognition and Machine Learning, Springer, ISBN 978-0-387-31073-2

Content Template	
Section Number	5.4
Section Title	Reporting
Introduction	In this section, we detail the last step in the network forensics process . After planning, collection and analysis comes reporting.
Content	Any conclusion or information about any breach or incident has to be properly written-up, reported and presented to higher management of an institution, to law enforcement agencies, or to a court of law. Some Security Incident and Event Management (SIEM) tools have such reporting capabilities. Even with auto-generated reports, the investigator will typically need to write a professional report detailing findings of the forensic process . It is a major responsibility and it has to be done with diligence . Any mistake might have severe consequences for the investigator, his institution, and others . The report produced must be easy to understand by nontechnical stakeholders , such as: lawyers and their assistants , corporate managers, human resources, judges, etc. The report has to be comprehensive, presentable, based on facts and entirely defensible. In general, it should be easy to understand, while maintaining professionalism.

Activity Template	
Number	5.1
Title	Write a report about the importance of Network evidence
Type	Reflection
Aim	Upon completion the student will be able to explain the value of Network evidence
Description	Using Google Scholar for scientific research, select a recent scientific paper/article or book that describes the challenges around Network Evidence. Related to Section 5.1
Timeline	1.5 hours to identify and read the article 1.5 hours to write the report Total 3 Hours
Assessment	The instructor grades the reports and return them to students.

Activity Template	
Number	5.2
Title	Investigate Network Based Evidence sources
Type	Research
Aim	Upon completion the student will be able to list and differentiate between various network based evidence sources
Description	Go to Section 1.4.1 and write a couple of lines for each source listed in the section outlining your expectations on how this source would be used in a forensic investigation.
Timeline	2 hours
Assessment	The instructor grades the reports and return them to students.

Activity Template	
Number	5.3
Title	Network Evidence Analysis: Sniffing wireless traffic using TCPDump
Type	Practical Experience
Aim	Upon completion students will be able to use tcpdump to improve the student's skills of network evidence examination and analysis. In order to help the students build a strong foundation in the network forensics concepts and practices, it is important for the students to do hands-on practice.
Description	TCPDump is a common packet sniffer and analyzer, runs in command line, intercepts and displays packets being transmitted over a network. It captures, displays, and stores all forms of network traffic in a variety of output formats. It will print packet data such as timestamp, protocol, source and destination hosts and ports, flags, options, and sequence numbers. Use TCPDump to sniff network traffic and direct the output to a file (pcap) that can be stored as long term backup or as a source for analysis by another tool. Run the command with 3 different options to explore its capability. Submit a report and screenshots. Related to section: 5.2.1 Log Managers
Timeline	5 hours
Assessment	The instructor grades the reports and return them to students.

Activity Template	
Number	5.4
Title	Investigate Log Managers
Type	Practical Experience
Aim	Upon completion students will be able to setup a log manager/server and connect it to log source
Description	Download syslog-ng and install it on your Linux machine. Connect to any available network device and start to populate the syslog server with logs from that source. Write a report about visibility and filtration capabilities of the tool and include appropriate screen shots. Related to: Content 5.2.2 Log Manager Examples
Timeline	5 Hours
Assessment	The instructor grades the reports and returns them to students.

Activity Template	
Number	5.5
Title	Explore Security Incident and Event Management (SIEM) Tools
Type	Practical Experience
Aim	Gain Hands-on experience with a SIEM tool and explore its features.
Description	Download AlienVault open-source SIEM and install it on your machine. Connect to any available network device and log servers and monitor network logs and dashboards. Write a report about visibility and alarm capabilities of the tool alongside appropriate screen shots. Related section 5.3.3
Timeline	5 Hours
Assessment	The instructor grades the reports and return them to students.

Think Template (MCQs)	
Number	5.1
Title	Evidence collection
Type	Multiple Choice: • Choose the correct answer
Question	Which of the following logs successful/failed login attempts for all devices within its authentication system a) Induction coils b) DHCP Servers c) DNS/Name Servers d) Authentication Servers
Answers	d) Authentication Servers

Think Template (MCQs)	
Number	5.1
Title	Evidence collection
Type	Multiple Choice: • Choose the correct answer
Question	Which of the following contains routing tables and may function as packet filters? a) Routers b) Firewalls c) TCP d) tcpdump
Answers	a) Routers

Think Template (MCQs)	
Number	5.1
Title	Evidence collection
Type	Multiple Choice: • Choose the correct answer
Question	Which of the following is a tool for capturing, filtering, and analyzing traffic? a) Routers b) TCP c) Switchs d) tcpdump
Answers	d) tcpdump

Think Template (MCQs)	
Number	5.2
Title	Evidence Examination
Type	Multiple Choice: • Choose the correct answer
Question	Which of the following is not true of log managers: i) Should keep logs for as long as possible j) Require considerable amounts of storage k) Should be capable of receiving network logs without delay l) Carry out log analysis
Answers	d)

Think Template (MCQs)	
Number	5.3.4
Title	Security Incident and Event Management (SIEM) Technologies
Type	Multiple Choice: • Choose the correct answer
Question	Which of the following is a technology used in SIEM tools: a) Artificial intelligence . b) Machine learning c) Statistical analysis d) Behaviour analysis e) All of the above
Answers	e) All of the above

Extra Template	
Number	5.1
Title	SIEM Tools Ranking
Topic	5.3.3 Security Incident and Event Management (SIEM) Tools
Type	Go to Gartner web site and find out the latest ranking of the SIEM tools. Prepare a report comparing the top 5 at the time of access. Download, install, configure, run, extract security events and add them to the report • URL: https://www.gartner.com/