SHRI VILEPARLE KELAVANI MANDAL'S

SHRI BHAGUBHAI MAFATLAL POLYTECHNIC

Program : Diploma in Information Technology

INTERNET SECURITY (ISS190915) PT2 APRIL 2024 QUESTION BANK

1. **Differentiate between DOS and DDOS . List at least two protocol failures that can cause these attacks.**

DOS	DDOS
DOS stands for denial-of-service attack	DDOS stands for distributed denial of service attacks
In DOS attack single system targets the victim's system	In DDOS attack multiple systems attacks the victim's system
Victim PC is loaded from the packet of data sent from a single location	Victim PC is loaded from a packet of data sent from multiple location
DOS attack is slower as compared to DDOS attack	DDOS attack is faster than compared to DOS attack
DOS attack can be blocked easily as only one system is used	It is difficult to block DDOS attack as multiple devices are sending packets and attacking from multiple locations
In DOS attack only a single device is used with DOS attack tools	In DDOS attack Bots are used to attack at the same time
DOS attacks are easy to trace	DDOS attacks are Difficult to trace
Volume of traffic is less in DOS attack as compared to DDOS attack	DDOS attack allows the attacker to send massive volumes of traffic to the victims' network.

Protocol failures which result in this attacks:

- TCP protocol which can lead to SYN Flooding attack
- ICMP protocol which might lead the victim to respond with 'Host Unreachable' message
- UDP

2. **Discuss password cracking with the help of Brute force attack/list and explain working of any two tools used for password cracking.**

Password cracking refers to the process of extracting passwords from the associated password hash.
A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

Two tools Used:

- Cain and Abel
  Cain and Abel is a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks

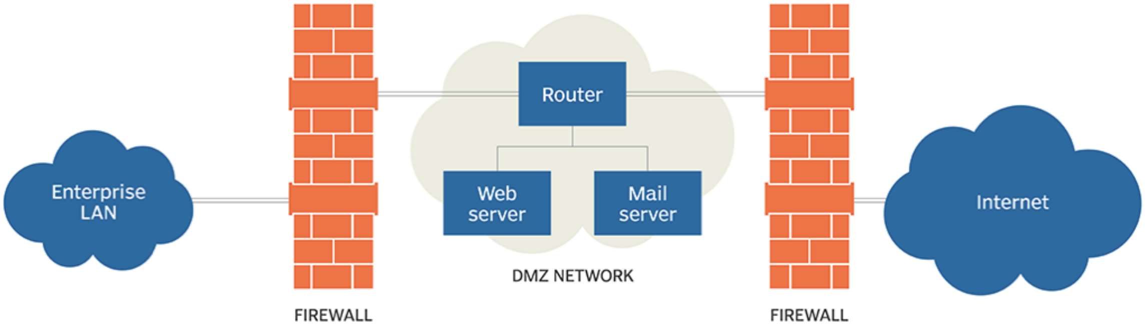
- Brutus Password Cracker

Brutus password cracker uses the Dictionary Attack for retrieving passwords. You can use the software for cracking simple passwords. The desktop application works only on Windows operating systems. Supports FTP, HTTP, POP3, SMB, Telnet, NetBus, IMAP, NNTP, and other platforms

3. Differentiate between Active and passive attacks.

ACTIVE ATTACK	PASSIVE ATTACK
In active attack , an attacker tries to modify the content of the messages	In passive attack, an attacker observes the messages , copy them and may use them for malicious purposes
In Active attack, Information is modified	In Passive attack, information remains unchanged
Active Attack is dangerous for Integrity as well as Availability.	Passive Attack is dangerous for Confidentiality.
In Active attack, Attention is to be paid on detection.	In Passive attack, Attention is to be paid on prevention.
In Active Attack, system is damaged.	In Passive Attack, system has no impact.
Victim gets informed in active attack.	Victim does not get informed in passive attack.
System Resources can be changed in active attack.	System Resources are not changed in passive attack.

4. illustrate the association between firewall Demilitarized zones with the help of neat diagram. CO2



- In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet. DMZs are also known as perimeter networks or screened subnetworks.
- Any service provided to users on the public internet should be placed in the DMZ network. External-facing servers, resources and services are usually located there. Some of the most common of these services include web, email, domain name system, File Transfer Protocol and proxy servers.
- Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet.

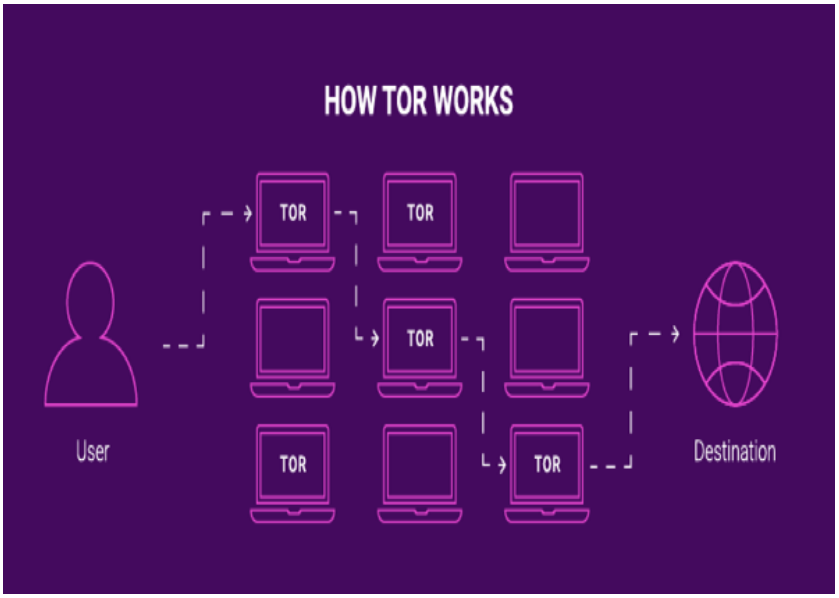
5. Define 'Anonymity on the Internet '.Explain the working of TOR ,ONION ,MIXNET anonymizer with the help of neat diagram. CO2

Anonymity means that the real author of a message is not shown. Anonymity can be implemented to make it impossible or very difficult to find out the real author of a message. A common variant of anonymity is pseudonymity, where another name than the real author is shown.

Tor (formerly an acronym for "The Onion Router") is often touted as a way to browse the web anonymously. From human rights activists evading oppressive governments to drug dealers selling through online marketplaces, Tor is a popular way to gain significantly more anonymity than you would normally have online.

Working of TOR: -

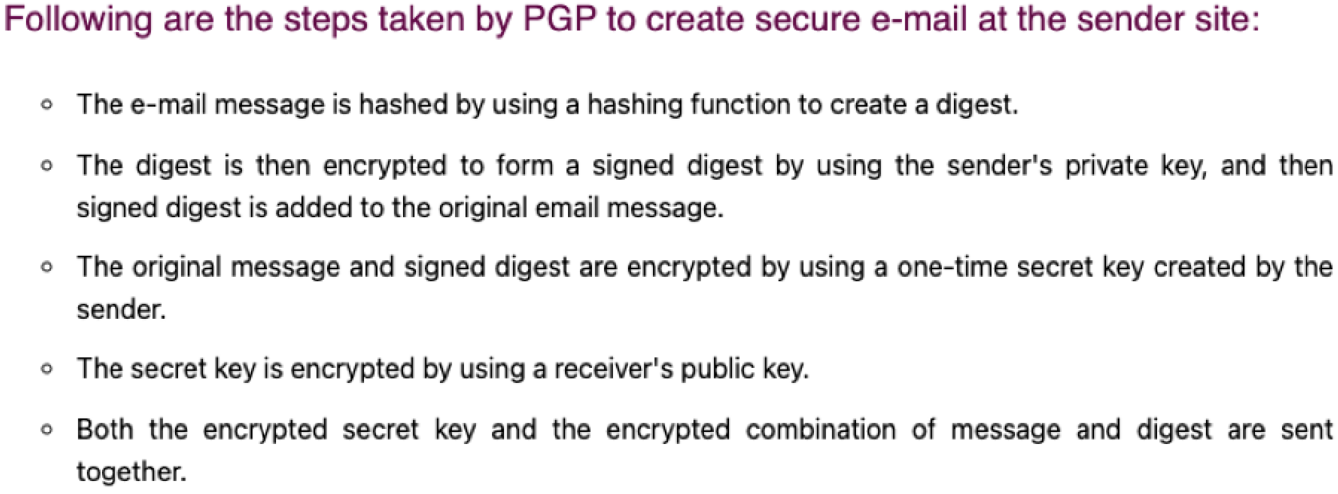
- To anonymize Internet usage, Tor routes traffic through multiple randomly-chosen relay servers before accessing the destination website.
- There are over 7,000 of these servers, which mostly belong to volunteers.
- The request is encrypted multiple times, so the relay servers only know the previous relay and the next relay, but not the request contents or the full circuit.
- The network request finally exits the Tor network at an exit node. From the website's perspective, you are browsing directly from the exit node.



6. justify how PGP achieves security for EMAIL communication. CO1

- PGP stands for Pretty Good Privacy (PGP).
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.

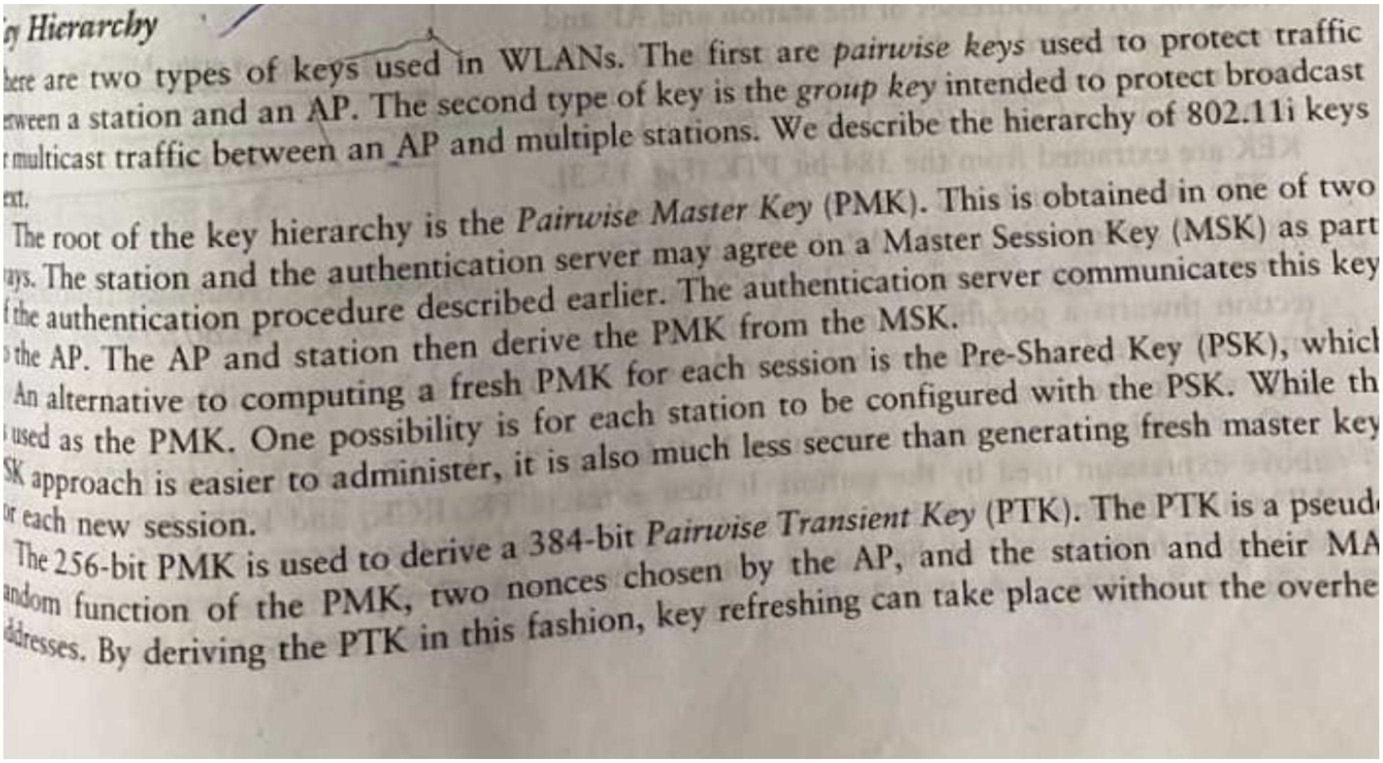
Email is a prime attack method for cyber criminals who can easily forge messages using a victim's name or identity . PGP aims to solve this and enhance email security by encrypting the data to make the communication method private



Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

7. With the help of block diagram. Explain how each key is derived in 802.11i and the usage to which the keys are applied.



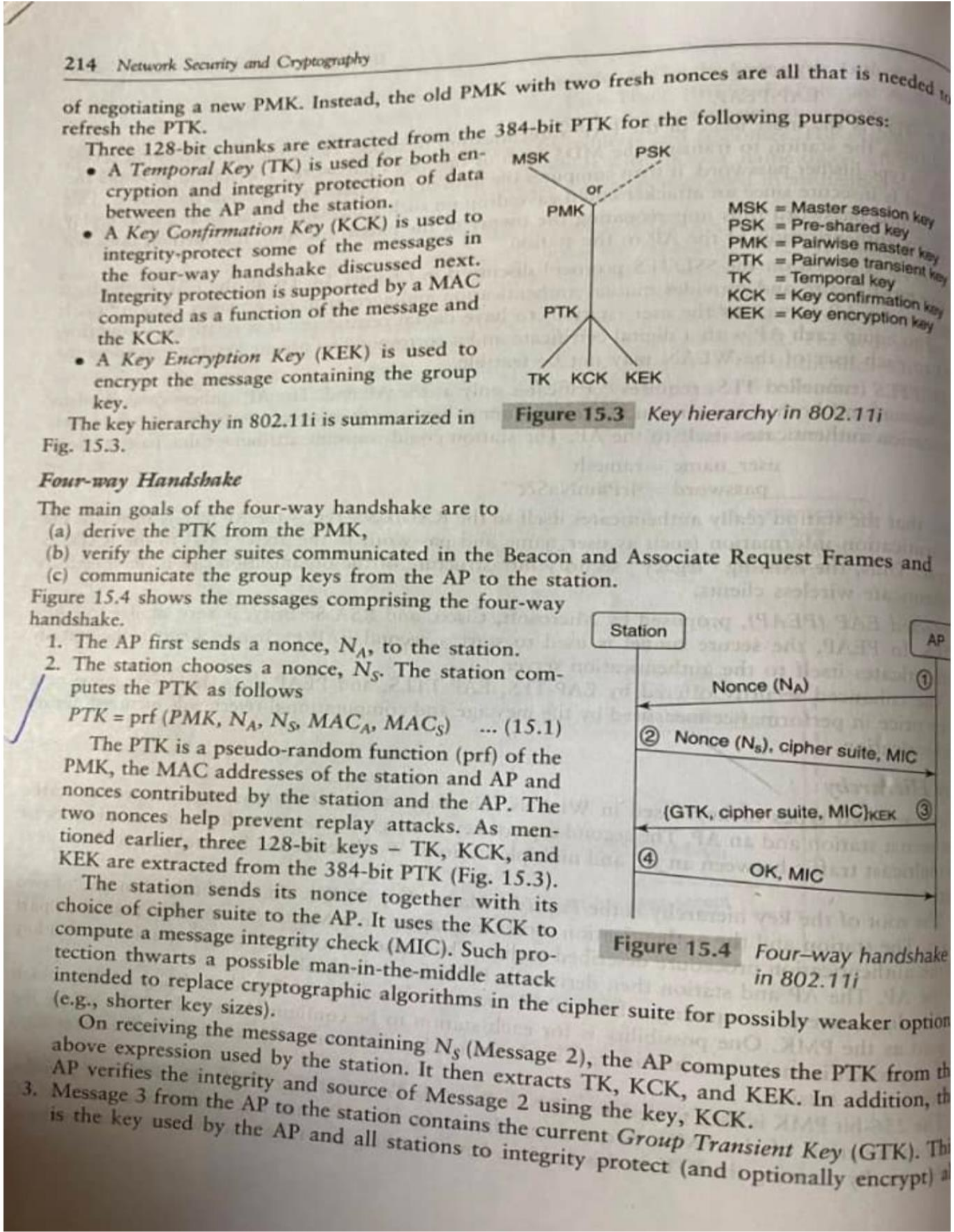
y Hierarchy

here are two types of keys used in WLANs. The first are *pairwise keys* used to protect traffic tween a station and an AP. The second type of key is the *group key* intended to protect broadcast r multicast traffic between an AP and multiple stations. We describe the hierarchy of 802.11i keys xt.

The root of the key hierarchy is the *Pairwise Master Key* (PMK). This is obtained in one of two ays. The station and the authentication server may agree on a Master Session Key (MSK) as part f the authentication procedure described earlier. The authentication server communicates this key the AP. The AP and station then derive the PMK from the MSK.

An alternative to computing a fresh PMK for each session is the Pre-Shared Key (PSK), whicl used as the PMK. One possibility is for each station to be configured with the PSK. While th SK approach is easier to administer, it is also much less secure than generating fresh master key r each new session.

The 256-bit PMK is used to derive a 384-bit *Pairwise Transient Key* (PTK). The PTK is a pseud andom function of the PMK, two nonces chosen by the AP, and the station and their MA ddresses. By deriving the PTK in this fashion, key refreshing can take place without the overhe



214 *Network Security and Cryptography*

of negotiating a new PMK. Instead, the old PMK with two fresh nonces are all that is needed t refresh the PTK.

Three 128-bit chunks are extracted from the 384-bit PTK for the following purposes:

- A *Temporal Key* (TK) is used for both encryption and integrity protection of data between the AP and the station.
- A *Key Confirmation Key* (KCK) is used to integrity-protect some of the messages in the four-way handshake discussed next. Integrity protection is supported by a MAC computed as a function of the message and the KCK.
- A *Key Encryption Key* (KEK) is used to encrypt the message containing the group key.

The key hierarchy in 802.11i is summarized in Fig. 15.3.

Figure 15.3 *Key hierarchy in 802.11i*

Four-way Handshake

The main goals of the four-way handshake are to
(a) derive the PTK from the PMK,
(b) verify the cipher suites communicated in the Beacon and Associate Request Frames and
(c) communicate the group keys from the AP to the station.

Figure 15.4 shows the messages comprising the four-way handshake.

1. The AP first sends a nonce, N_A, to the station.
2. The station chooses a nonce, N_S. The station computes the PTK as follows

$$PTK = prf\ (PMK, N_A, N_S, MAC_A, MAC_S) \quad ... (15.1)$$

The PTK is a pseudo-random function (prf) of the PMK, the MAC addresses of the station and AP and nonces contributed by the station and the AP. The two nonces help prevent replay attacks. As mentioned earlier, three 128-bit keys – TK, KCK, and KEK are extracted from the 384-bit PTK (Fig. 15.3).

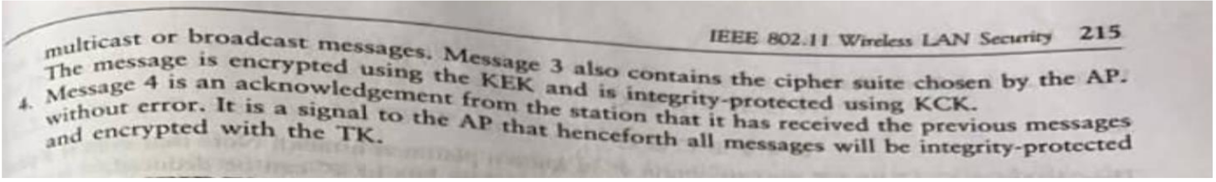
The station sends its nonce together with its choice of cipher suite to the AP. It uses the KCK to compute a message integrity check (MIC). Such protection thwarts a possible man-in-the-middle attack intended to replace cryptographic algorithms in the cipher suite for possibly weaker option (e.g., shorter key sizes).

On receiving the message containing N_S (Message 2), the AP computes the PTK from th above expression used by the station. It then extracts TK, KCK, and KEK. In addition, th AP verifies the integrity and source of Message 2 using the key, KCK.

3. Message 3 from the AP to the station contains the current *Group Transient Key* (GTK). Thi is the key used by the AP and all stations to integrity protect (and optionally encrypt) a

Station
AP
① Nonce (N_A)
② Nonce (N_S), cipher suite, MIC
(GTK, cipher suite, MIC)KEK ③
④ OK, MIC

Figure 15.4 *Four–way handshake in 802.11i*



IEEE 802.11 *Wireless LAN Security* 215

multicast or broadcast messages. Message 3 also contains the cipher suite chosen by the AP. The message is encrypted using the KEK and is integrity-protected using KCK.

4. Message 4 is an acknowledgement from the station that it has received the previous messages without error. It is a signal to the AP that henceforth all messages will be integrity-protected and encrypted with the TK.

8. Explain the working of following tools a) Autopsy b) COFFEE. C)Encase .CO1

A] Autopsy: -

Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in the sleuth kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

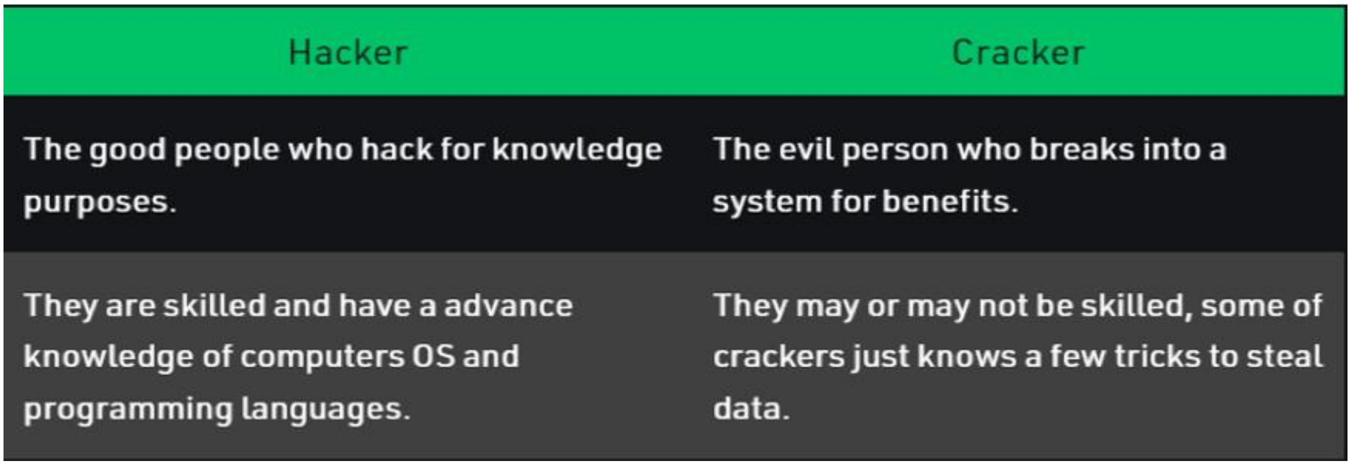
B] COFEE: -

The toolkit acts as an automated forensic tool during a live analysis. It contains more than 150 features and a graphical user interface that guides an investigator through data collection and examination and helps generate reports after extraction. Password decryption, internet history recovery, and other data collection forms are all included in the toolkit.

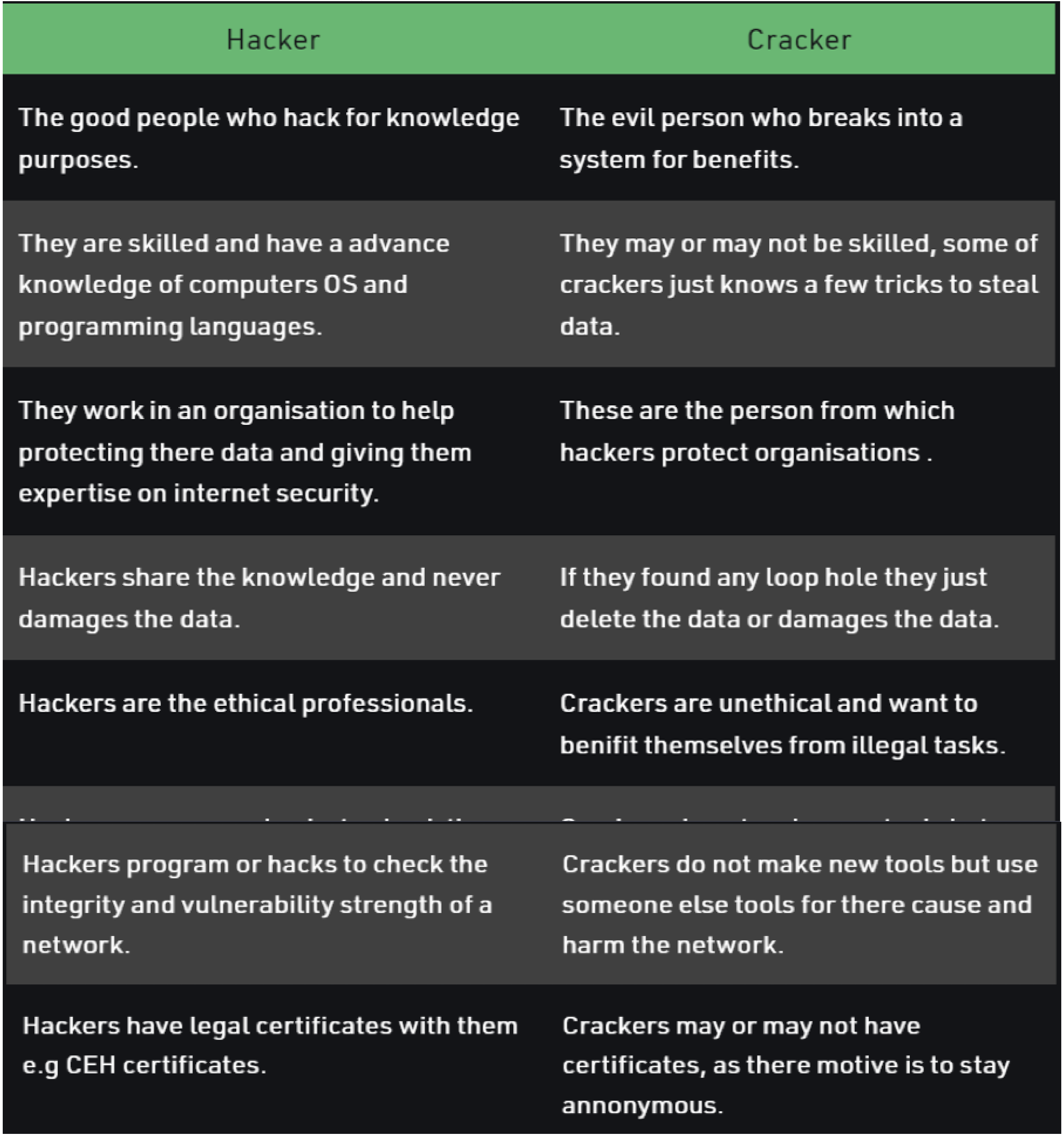
C] Encase: -

Encase is traditionally used in forensics to recover evidence from seized hard drives. Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

9. Differentiate between hacker and cracker? Compare white hat ,black hat and grey hat hacker CO1

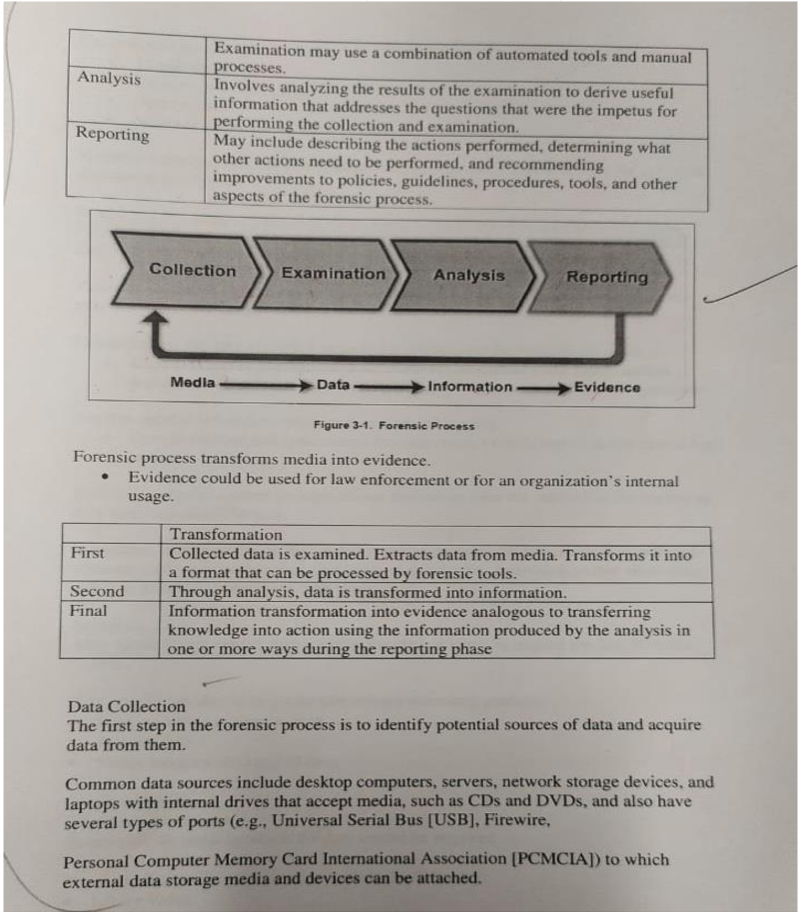


Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.



Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have a advance knowledge of computers OS and programming languages.	They may or may not be skilled, some of crackers just knows a few tricks to steal data.
They work in an organisation to help protecting there data and giving them expertise on internet security.	These are the person from which hackers protect organisations .
Hackers share the knowledge and never damages the data.	If they found any loop hole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benifit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for there cause and harm the network.
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as there motive is to stay annonymous.

10. With the help of a diagram flowchart explain the steps involved in digital forensics. CO1



	Examination may use a combination of automated tools and manual processes.
Analysis	Involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
Reporting	May include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

Figure 3-1. Forensic Process

Forensic process transforms media into evidence.

- Evidence could be used for law enforcement or for an organization's internal usage.

	Transformation
First	Collected data is examined. Extracts data from media. Transforms it into a format that can be processed by forensic tools.
Second	Through analysis, data is transformed into information.
Final	Information transformation into evidence analogous to transferring knowledge into action using the information produced by the analysis in one or more ways during the reporting phase

Data Collection
The first step in the forensic process is to identify potential sources of data and acquire data from them.

Common data sources include desktop computers, servers, network storage devices, and laptops with internal drives that accept media, such as CDs and DVDs, and also have several types of ports (e.g., Universal Serial Bus [USB], Firewire,

Personal Computer Memory Card International Association [PCMCIA]) to which external data storage media and devices can be attached.

The digital forensic process has the following 4 basic stages.

1. Collection – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
2. Examination - During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.
3. Analysis – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.
4. Reporting – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

11. Explain war driving? what are the tools used to carry out war driving. CO2

Wardriving consists of physically searching for wireless networks with vulnerabilities and mapping the wireless access point.

Wardrivers use hardware and software to find particular Wi-Fi signal in a particular area. Once such networks are located, war drivers will record the location and submit the information to third party websites and apps.

Three primary reasons for wardriving:

- To Steal personal and banking information
- To use vulnerable network for criminal activities
- to find security flaws of a network

Hardware and Software Tools for WarDriving

1. Hardware Tools for WarDriving:

There are several hardware tools are required to perform Wardriving.

A mobile device: This is a basic prerequisite for performing wardriving. You need a mobile computing platform like laptops, tablets, smartphones, or any other device like Raspberry Pi. These are used to subvert encryption and manage the overall process.

Wireless network card antenna: This is the most critical component of a wardriving setup. Wardrivers may opt to use a built-in antenna and card, or they can go for additional hardware to increase the scanning power of the device.

GPS System: The GPS system is used to determine the exact location of the Wi-Fi router that has been located. Many of the wardriving devices have built-in GPS capabilities.

2. Software Tools for Wardriving:

WiGLE: WiGLE is Wireless Geographic Logging Engine is a website where users can upload hotspot data like GPS coordinates, SSID, MAC Address to discover the encryption type that is used on the hotspot.

openBmap: It is a free and open map of the wireless communicating objects like Bluetooth, Wi-Fi, cellular antennae. It provides tools to mutualize data, create and access this map.

Geomena: It is an open geodatabase of Wi-Fi access points that are meant to be used for geolocation. The API provides a way to add data programmatically.

Feature	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)
Security Strength	Weak. Vulnerable to various attacks, easily compromised.	Stronger. Provides better security features and encryption.
Encryption	Relies on the RC4 stream cipher with 40/64-bit or 104/128-bit keys.	Initially used TKIP (Temporal Key Integrity Protocol) with RC4; later versions use AES (Advanced Encryption Standard).
Key Management	Uses static keys which are manually configured.	Offers dynamic key generation and distribution using protocols like WPA-PSK (Pre-Shared Key) or WPA-Enterprise with authentication servers.

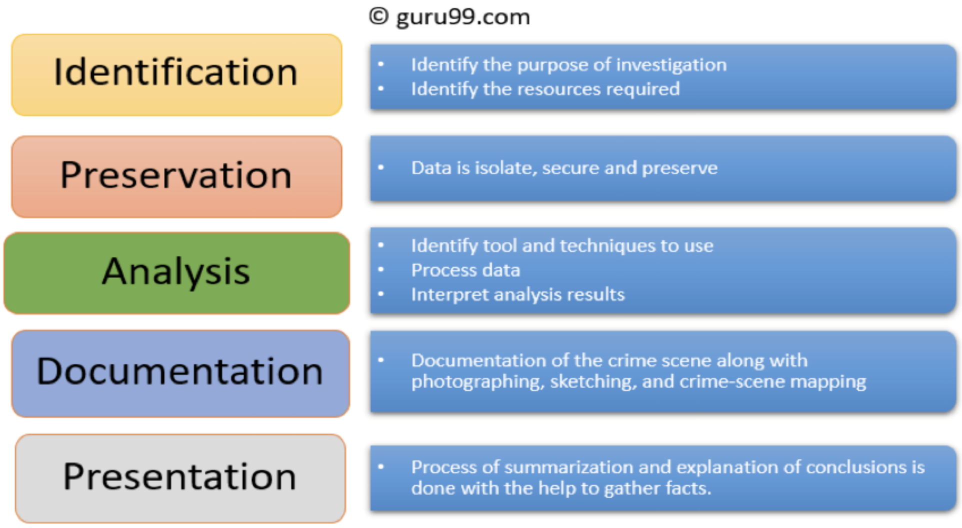
Authentication	Open system authentication or shared key authentication.	Supports more robust authentication methods like 802.1X/EAP (Extensible Authentication Protocol).
Vulnerabilities	Susceptible to various attacks, including IV (Initialization Vector) attacks and key recovery attacks.	Addresses many vulnerabilities of WEP, including better encryption and stronger key management.
Compatibility	Widely supported but largely deprecated due to security weaknesses.	Standardized as a replacement for WEP; backward-compatible with WEP devices.
Standards Compliance	Defined under the IEEE 802.11 standard.	Defined under the IEEE 802.11i standard.
Versions	No major versions; only minor revisions.	Evolved through various iterations: WPA, WPA2, and WPA3.
Usability	Simple setup but lacks robust security.	More complex setup due to additional security features but provides better protection.

12. Compare WEP and WAP protocols. CO2

13. Define the term cyber forensics and describe the steps involved in it.

Forensics is the process of applying scientific knowledge for the collection processing and analyzing to present evidence before the court.

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally.


© guru99.com
Identification
Identify the purpose of investigation
Identify the resources required
Preservation
Data is isolate, secure and preserve
Analysis
Identify tool and techniques to use
Process data
Interpret analysis results
Documentation
Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation
Process of summarization and explanation of conclusions is done with the help to gather facts.

Steps involved in cyber forensics:

1. Identification: The first step of cyber forensics experts are to identify what evidence is present, where it is stored, and in which format it is stored.
2. Preservation: After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
3. Analysis: After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files, verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
4. Documentation: Now after analyzing data a record is created. This record contains all the recovered and available(not deleted) data which helps in recreating the crime scene and reviewing it.
5. Presentation: This is the final step in which the analyzed data is presented in front of the court to solve cases along with the chain of custody.

14. Explain chain of custody as applied to digital forensics. CO1

Chain of custody indicates the collection, sequence of control, transfer and analysis. It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
It demonstrates trust to the courts and to the client that the evidence has not tampered.
Any break in the chain of custody makes the evidence inadmissible in the court. The chain of custody must include the description of evidence and documented history of each evidence transfer.

Chain of Custody Process
In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.

stages of the chain of custody:

Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.

Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.

Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.

Reporting: This is the documentation phase of the Examination and Analysis stage.

15. Describe Ten commandments of Ethical Hacking explain each in Brief

1. Thou shalt set thy goals

An ethical hacker should set simple goals, such as finding unauthorized wireless access points or obtaining information from a wired network system. In any case, the goals should be articulate and well communicated.

2. Thou shalt plan thy work, lest thou go off course

Ethical hackers are bound by constraints. Consequently, it is important to develop a strategy plan which should include identifying the networks to test, specifying the testing interval, specifying the testing process, and obtaining approval of the plan.

3. Thou shalt obtain permission

Written permission is required and should state that an ethical hacker is authorized to perform a test according to the plan. It should also say that the organization will provide legal and organizational support in case criminally charges or lawsuits arise. This is conditional on staying within the bounds of the approved plan.

4. Thou shalt work ethically

An ethical hacker is bound to confidentiality and non-disclosure of information they may uncover. Ethical hackers must also be compliant with their organization's governance and local laws. An ethical hack must not be performed when the company policy or the law for that matter, explicitly forbids it.

5. Thou shalt keep records

Patience and thoroughness are attributes of a good ethical hacker. A hallmark of ethical hacker professionalism is keeping adequate records to support findings. The date and details regarding each test, whether or not they were successful, should be logged and recorded and a duplicate copy of the log book should be kept.

6. Thou shalt respect the privacy of others

An ethical hacker must not abuse their authority. Ethical hackers must snoop into confidential corporate records or private lives. The information that is uncovered should be treated with the same care one would give to their own personal information.

7. Thou shalt do no harm

The actions of an ethical hacker may have unplanned repercussions. It is easy to get caught up in the work and cause a denial of service or trample on someone else's rights. It is important to stick to the original plan.

8. Thou shalt use a scientific process

The work of an ethical hacker should adopt an empirical method. An empirical method will help set quantifiable goals, develop consistent and repeatable tests, and provide tests that are valid in the future.

9. Thou shalt not covet thy neighbor's tools

Ethical hackers will always discover new tools to help them get their job done. Tools are abundant on the Internet and more are coming out all the time. The temptation to grab them all is fierce. Although it is possible to use all of the tools that are available, it is recommended that an ethical hacker choose one and stick with it.

10. Thou shalt report all thy findings

Ethical hackers should plan to report any high-risk vulnerabilities discovered during testing as soon as they are found. Reports are one way for the organization to determine the completeness and thoroughness of the work of an ethical hacker and provides a means for peers to review methodologies, findings, analysis, and conclusions.

16. With the help of a neat diagram explain the working of Tarzan anonymous network.

Tarzan is a peer-to-peer anonymizing network layer which was introduced in 2002.

It is a peer-to-peer anonymous IP network overlay. Because it provides IP service, Tarzan is general-purpose and transparent to applications. Organized as a decentralized peer-to-peer overlay, Tarzan is fault-tolerant, highly scalable, and easy to manage.

Architecture n design:

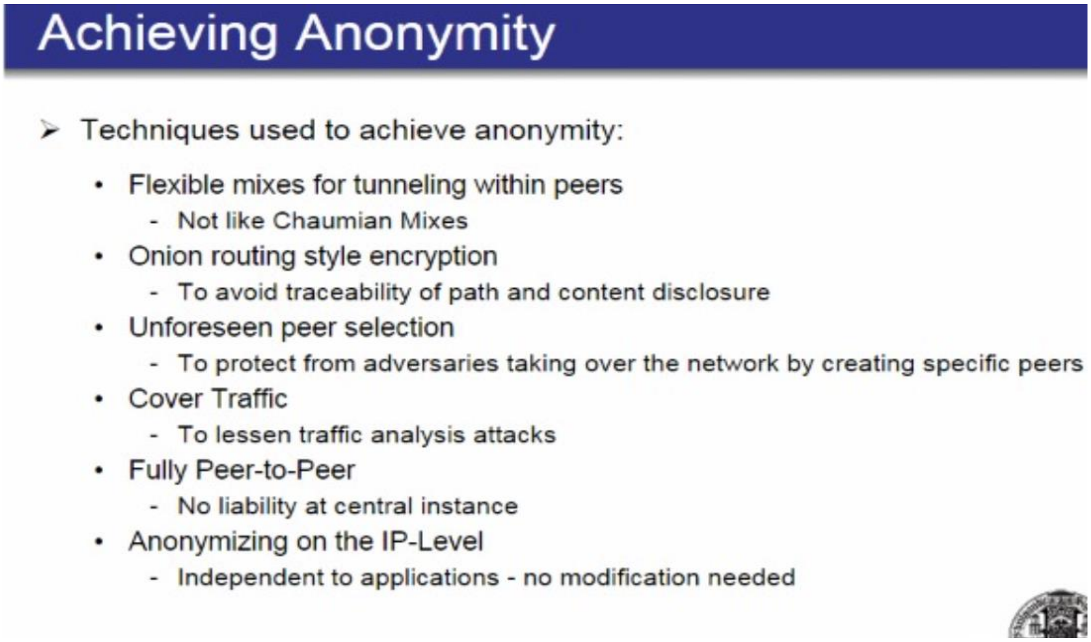
- Layered Encryption
- Peer discovery
- Mimic selection
- Tunnel setup
- Tunnel failure and reconstruction
- Cover traffic

Techniques by which Tarzan achieves anonymity:

- Flexible mixes for tunnelling within peers
- Onion routing style encryption
- Unforeseen peer selection
- Cover traffic
- Anonymizing on IP level

Tarzan achieves its anonymity with layered encryption and multi-hop routing. A message initiator chooses a path of peers pseudo-randomly through a restricted topology in a way that adversaries cannot easily influence.

Cover traffic prevents a global observer from using traffic analysis to identify an initiator. Protocols toward unbiased peer-selection offer new directions for distributing trust among untrusted entities.Tarzan provides anonymity to either clients or servers, without requiring that both participate. In both cases, Tarzan uses a network address translator (NAT) to bridge between Tarzan hosts and oblivious Internet hosts.Measurements show that Tarzan imposes minimal overhead over a corresponding non-anonymous overlay route.



Achieving Anonymity

➢ Techniques used to achieve anonymity:

- Flexible mixes for tunneling within peers
  - Not like Chaumian Mixes
- Onion routing style encryption
  - To avoid traceability of path and content disclosure
- Unforeseen peer selection
  - To protect from adversaries taking over the network by creating specific peers
- Cover Traffic
  - To lessen traffic analysis attacks
- Fully Peer-to-Peer
  - No liability at central instance
- Anonymizing on the IP-Level
  - Independent to applications - no modification needed

17. **Explain file carving, tools for password cracking (any two) CO1**

18. **Explain working of Wireshark and Burp suite and their usage CO1**

Wireshark:

1. Packet Capture: Wireshark captures packets from the network interface of a computer or device. It can capture packets from Ethernet, Wi-Fi, Bluetooth, and other network interfaces.
2. Protocol Analysis: Wireshark displays captured packets in a user-friendly interface, allowing users to analyze network traffic at the protocol level.
3. Packet Filtering: Users can apply filters to focus on specific types of traffic, such as HTTP, TCP, UDP, or packets to or from specific IP addresses.
4. Packet Decoding: Wireshark decodes packet contents, including headers and payloads, for various network protocols such as TCP, UDP, IP, HTTP, DNS, and more.
5. Packet Inspection: Users can inspect packet details, including source and destination addresses, port numbers, protocol versions, and packet timing.
6. Network Troubleshooting: Wireshark is commonly used for network troubleshooting, diagnosing network issues, analyzing performance problems, and identifying security threats.

Burp Suite:

1. Proxy Intercept: Burp Suite acts as a proxy between the user's browser and the target web application, intercepting HTTP/S requests and responses.
2. Request Modification: Users can modify intercepted requests before they are sent to the target server. This allows for testing various security aspects such as input validation, session management, and authentication mechanisms.
3. Repeater: Burp Suite's Repeater tool allows users to resend captured requests to the target server, making it easy to perform manual testing and observe the application's response to different inputs.
4. Intruder: The Intruder tool automates attacks such as brute force, dictionary, and fuzzing attacks by sending multiple variations of a request to the target server and analyzing the responses.
5. Scanner: Burp Suite Scanner automatically scans web applications for security vulnerabilities such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities.
6. Sequencer: The Sequencer tool analyzes the randomness and quality of session tokens or other pieces of data generated by the target application, helping to identify weaknesses in cryptographic implementations.
7. Spider: The Spider tool crawls the target web application, mapping out its structure and identifying potential entry points for further testing.

8. Extensibility: Burp Suite offers extensive extensibility through its support for custom scripts and plugins, allowing users to add new features or automate specific tasks according to their requirements.

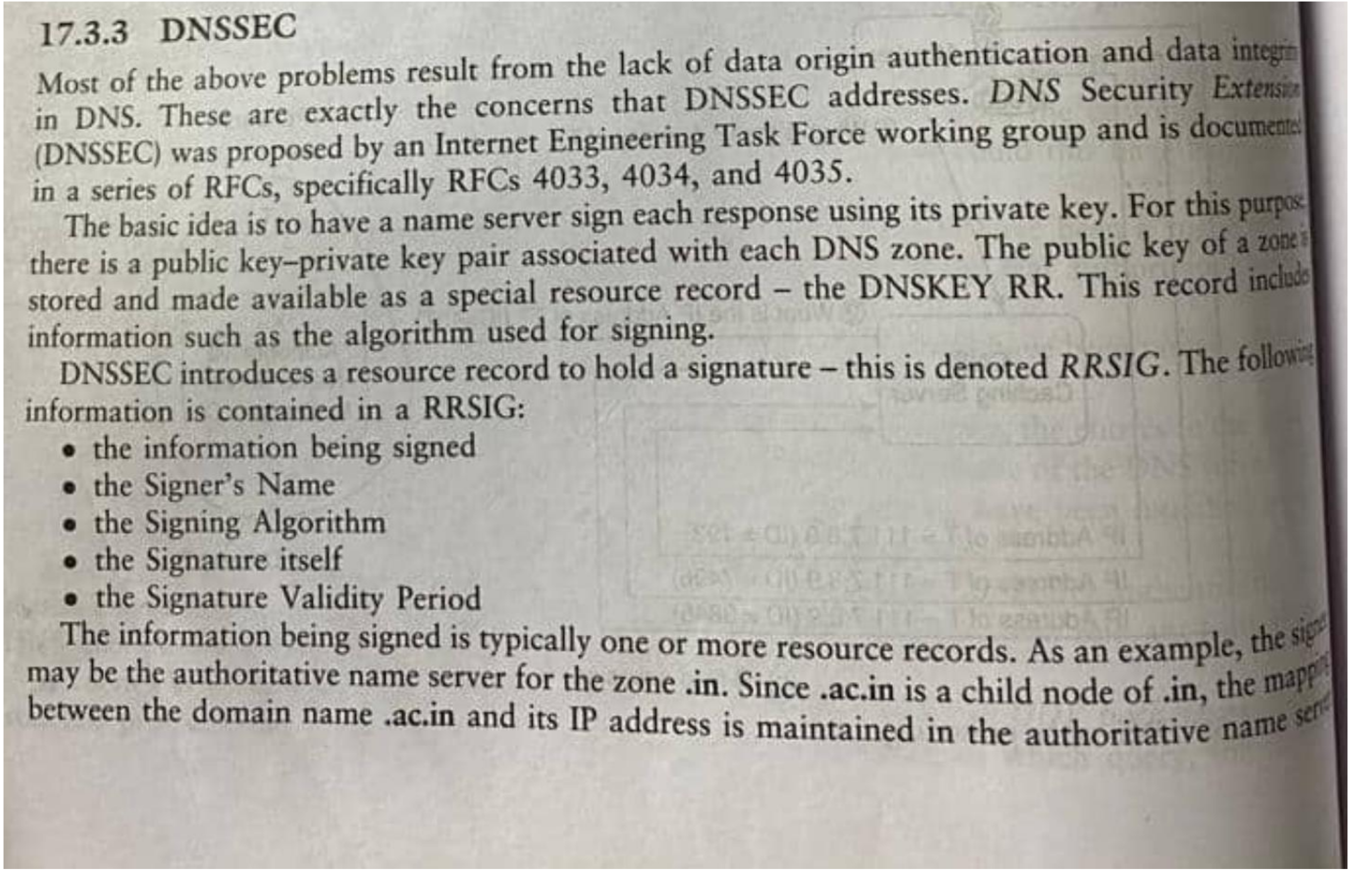
Uses of wireshark:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Uses of burpSuite:

- Testing workflow
  Burp lets you combine manual and automated techniques effectively, gives you complete control over all of the actions that Burp performs, and provides detailed information and analysis about the applications you are testing.
- Recon and analysis
  The Proxy tool lies at the heart of Burp's workflow. It lets you use Burp's browser to navigate the application, while Burp captures all relevant information and lets you easily initiate further actions. In a typical test, the recon and analysis phase involves the tasks described below.
- Vulnerability detection and exploitation
  After completing your recon and analysis of the target application, and any necessary configuration of Burp, you can begin probing the application for common vulnerabilities

19. Explain DNSSEC working pg242(Bernard) CO2



17.3.3 DNSSEC

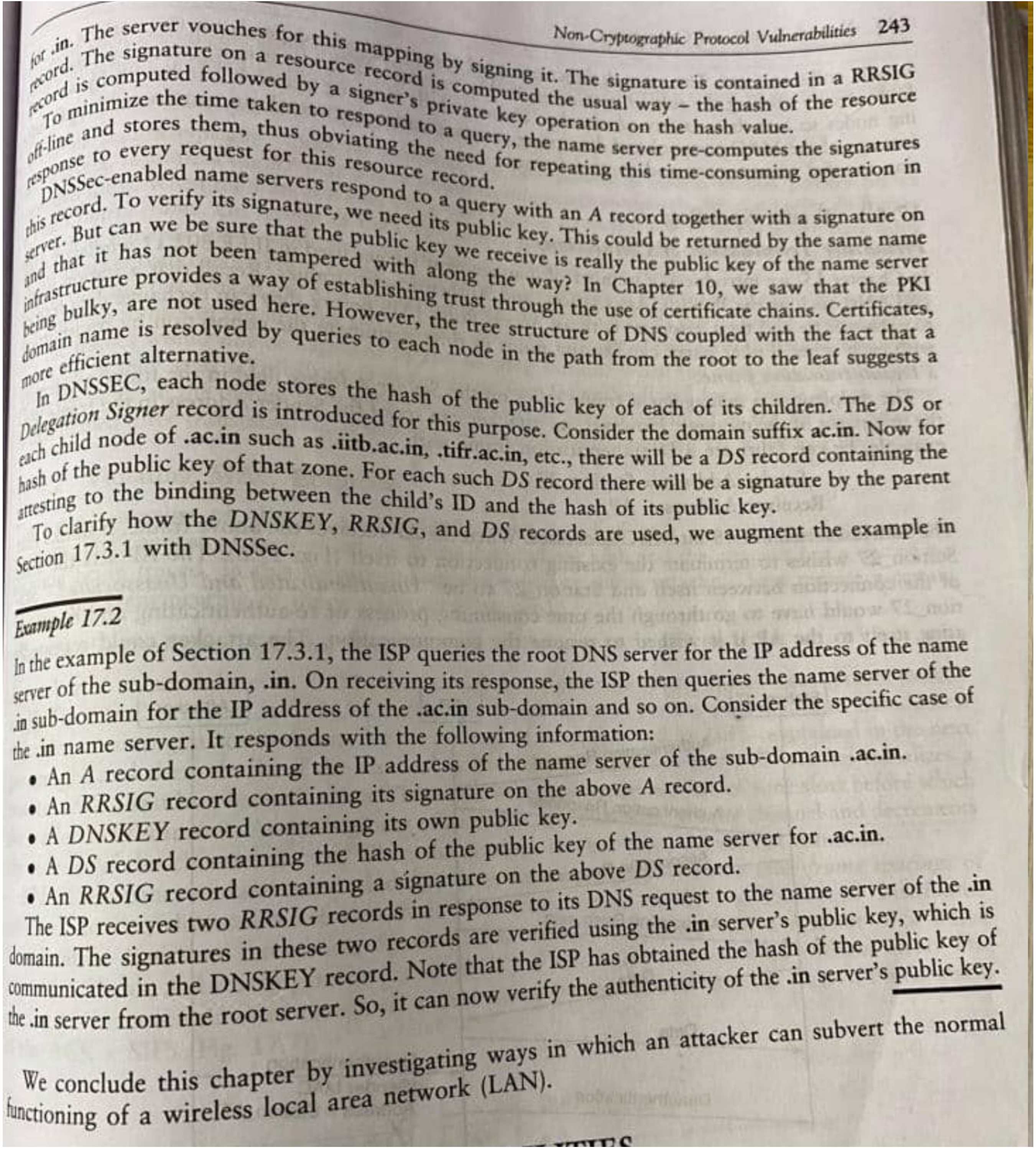
Most of the above problems result from the lack of data origin authentication and data integrity in DNS. These are exactly the concerns that DNSSEC addresses. *DNS Security Extensions* (DNSSEC) was proposed by an Internet Engineering Task Force working group and is documented in a series of RFCs, specifically RFCs 4033, 4034, and 4035.

The basic idea is to have a name server sign each response using its private key. For this purpose there is a public key–private key pair associated with each DNS zone. The public key of a zone is stored and made available as a special resource record – the DNSKEY RR. This record includes information such as the algorithm used for signing.

DNSSEC introduces a resource record to hold a signature – this is denoted *RRSIG*. The following information is contained in a RRSIG:

- the information being signed
- the Signer's Name
- the Signing Algorithm
- the Signature itself
- the Signature Validity Period

The information being signed is typically one or more resource records. As an example, the signer may be the authoritative name server for the zone **.in**. Since **.ac.in** is a child node of **.in**, the mapping between the domain name **.ac.in** and its IP address is maintained in the authoritative name server



for .in. The server vouches for this mapping by signing it. The signature is contained in a RRSIG record. The signature on a resource record is computed the usual way – the hash of the resource record is computed followed by a signer's private key operation on the hash value.

To minimize the time taken to respond to a query, the name server pre-computes the signatures off-line and stores them, thus obviating the need for repeating this time-consuming operation in response to every request for this resource record.

DNSSec-enabled name servers respond to a query with an *A* record together with a signature on this record. To verify its signature, we need its public key. This could be returned by the same name server. But can we be sure that the public key we receive is really the public key of the name server and that it has not been tampered with along the way? In Chapter 10, we saw that the PKI infrastructure provides a way of establishing trust through the use of certificate chains. Certificates, being bulky, are not used here. However, the tree structure of DNS coupled with the fact that a domain name is resolved by queries to each node in the path from the root to the leaf suggests a more efficient alternative.

In DNSSEC, each node stores the hash of the public key of each of its children. The *DS* or *Delegation Signer* record is introduced for this purpose. Consider the domain suffix **ac.in**. Now for each child node of **.ac.in** such as **.iitb.ac.in**, **.tifr.ac.in**, etc., there will be a *DS* record containing the hash of the public key of that zone. For each such *DS* record there will be a signature by the parent attesting to the binding between the child's ID and the hash of its public key.

To clarify how the *DNSKEY*, *RRSIG*, and *DS* records are used, we augment the example in Section 17.3.1 with DNSSec.

Example 17.2

In the example of Section 17.3.1, the ISP queries the root DNS server for the IP address of the name server of the sub-domain, **.in**. On receiving its response, the ISP then queries the name server of the **.in** sub-domain for the IP address of the **.ac.in** sub-domain and so on. Consider the specific case of the **.in** name server. It responds with the following information:

- An *A* record containing the IP address of the name server of the sub-domain **.ac.in**.
- An *RRSIG* record containing its signature on the above *A* record.
- A *DNSKEY* record containing its own public key.
- A *DS* record containing the hash of the public key of the name server for **.ac.in**.
- An *RRSIG* record containing a signature on the above *DS* record.

The ISP receives two *RRSIG* records in response to its DNS request to the name server of the **.in** domain. The signatures in these two records are verified using the **.in** server's public key, which is communicated in the DNSKEY record. Note that the ISP has obtained the hash of the public key of the **.in** server from the root server. So, it can now verify the authenticity of the **.in** server's public key.

We conclude this chapter by investigating ways in which an attacker can subvert the normal functioning of a wireless local area network (LAN).

20. State one vulnerability in the design of each of following protocols. Explain how the vulnerability may be exploited leading to an attack. a)TCP B)UDP C)ICMP D)IP E)ARP F)802.11 G)ETHERNET h)DNS .Is there a downside in fixing these vulnerabilities such as increased cost/complexity,reduced performance etc. if so explain How? . CO2

a) TCP:

- Vulnerability: TCP Sequence Number Prediction - An attacker might predict the sequence number in a TCP stream and inject packets that appear legitimate, potentially disrupting communication or hijacking sessions.
- Exploitation (Example - TCP SYN Flooding): An attacker sends a large number of SYN packets (connection initiation requests) with spoofed IP addresses. The target overflows its connection queue, denying service to legitimate connections.
- Downside of Fixing: Complex solutions like sequence number randomization add processing overhead, potentially impacting performance.

b) UDP:

- Vulnerability: Lack of built-in integrity checking - UDP doesn't guarantee data hasn't been tampered with during transmission.
- Exploitation (Example - DNS Spoofing): An attacker modifies DNS responses, redirecting traffic to malicious servers. Since UDP lacks integrity checks, the modification might go unnoticed.
- Downside of Fixing: Adding integrity checks to UDP would increase packet size and processing overhead, impacting performance for latency-sensitive applications.

c) ICMP:

- Vulnerability: ICMP messages are often unauthenticated, allowing attackers to spoof the source address.
- Exploitation (Example - Smurf Attack): An attacker sends large volumes of ICMP Echo Request (ping) packets with a spoofed source IP address of the target network. The target network gets flooded with replies from other hosts, overwhelming it.
- Downside of Fixing: Implementing ICMP authentication adds complexity and processing overhead, potentially impacting performance.

d) IP:

- Vulnerability: IP spoofing - An attacker can forge the source IP address in a packet, making it appear to come from a trusted source.
- Exploitation (Example - Man-in-the-Middle Attack): An attacker positions itself between two communicating parties, intercepts and modifies traffic while appearing legitimate to both.
- Downside of Fixing: Strict source address verification adds complexity to routers and might not be feasible for all network configurations, impacting scalability.

e) ARP (Address Resolution Protocol):

- Vulnerability: ARP Cache Poisoning - An attacker can send fake ARP replies, associating their MAC address with another device's IP address.
- Exploitation (Example - ARP Spoofing): An attacker intercepts traffic meant for another device.
- Downside of Fixing: Secure ARP (SARP) protocols introduce additional complexity and require wider adoption for effectiveness, impacting interoperability.

f) 802.11 (Wi-Fi):

- Vulnerability: Older encryption standards like WEP and WPA (TKIP) were vulnerable to cracking.
- Exploitation (Example - WEP Cracking): An attacker could capture Wi-Fi traffic and decrypt it using brute-force or other techniques.
- Downside of Fixing: Stronger encryption (WPA2/WPA3) requires more processing power on devices, potentially impacting battery life on mobile devices.

g) Ethernet:

- Vulnerability: Shared medium - All devices on a shared Ethernet segment can see all traffic, making it susceptible to eavesdropping.
- Exploitation (Example - Packet Sniffing): An attacker can capture network traffic using readily available tools.
- Downside of Fixing: Switching technology mitigates shared medium issues but adds cost and complexity to network infrastructure.

h) DNS:

- Vulnerability: DNS Cache Poisoning - An attacker can manipulate DNS records on a DNS server, causing users to be redirected to malicious websites.
- Exploitation (Example - DNS Cache Poisoning Attack): An attacker redirects users to phishing sites that steal credentials.

- Downside of Fixing: DNS Security Extensions (DNSSEC) improve security but require widespread adoption by DNS servers and resolvers, impacting interoperability.

21. Explain CHAIN OF CUSTODY. CO1

Chain of custody indicates the collection, sequence of control, transfer and analysis. It also documents details of each person who handled the evidence, date and time it was collected or transferred, and the purpose of the transfer.
It demonstrates trust to the courts and to the client that the evidence has not tampered.
Any break in the chain of custody makes the evidence inadmissible in the court. The chain of custody must include the description of evidence and documented history of each evidence transfer.

Chain of Custody Process
In order to preserve digital evidence, the chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.

stages of the chain of custody:

Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.

Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.

Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.

Reporting: This is the documentation phase of the Examination and Analysis stage.

22. List and explain various password cracking Tools.(any4) CO2

Password cracking tools are software programs designed to recover or bypass password security measures by systematically attempting different combinations of characters until the correct password is found. These tools are often used by security professionals for penetration testing and by attackers for malicious purposes. Here are four popular password cracking tools:

1. John the Ripper:

- John the Ripper is one of the oldest and most widely used password cracking tools. It supports various encryption algorithms and hash formats, making it versatile for cracking passwords stored in different formats, including Unix/Linux password hashes, Windows LM and NTLM hashes, and many others.
- John the Ripper utilizes both dictionary-based attacks, where it tries words from a predefined list, and brute-force attacks, where it systematically tries all possible combinations of characters, to crack passwords.
- It offers GPU acceleration support, allowing it to leverage the computational power of graphics processing units (GPUs) for faster password cracking.

2. Hashcat:

- Hashcat is a highly efficient password cracking tool known for its speed and support for multiple hashing algorithms, including MD5, SHA-1, SHA-256, bcrypt, and others.
- It supports various attack modes, including dictionary attacks, mask attacks (where specific patterns are defined for password generation), and hybrid attacks (combining dictionary and brute-force techniques).
- Hashcat can utilize both CPU and GPU resources for password cracking, making it suitable for cracking complex passwords within a reasonable timeframe.

3. Medusa:

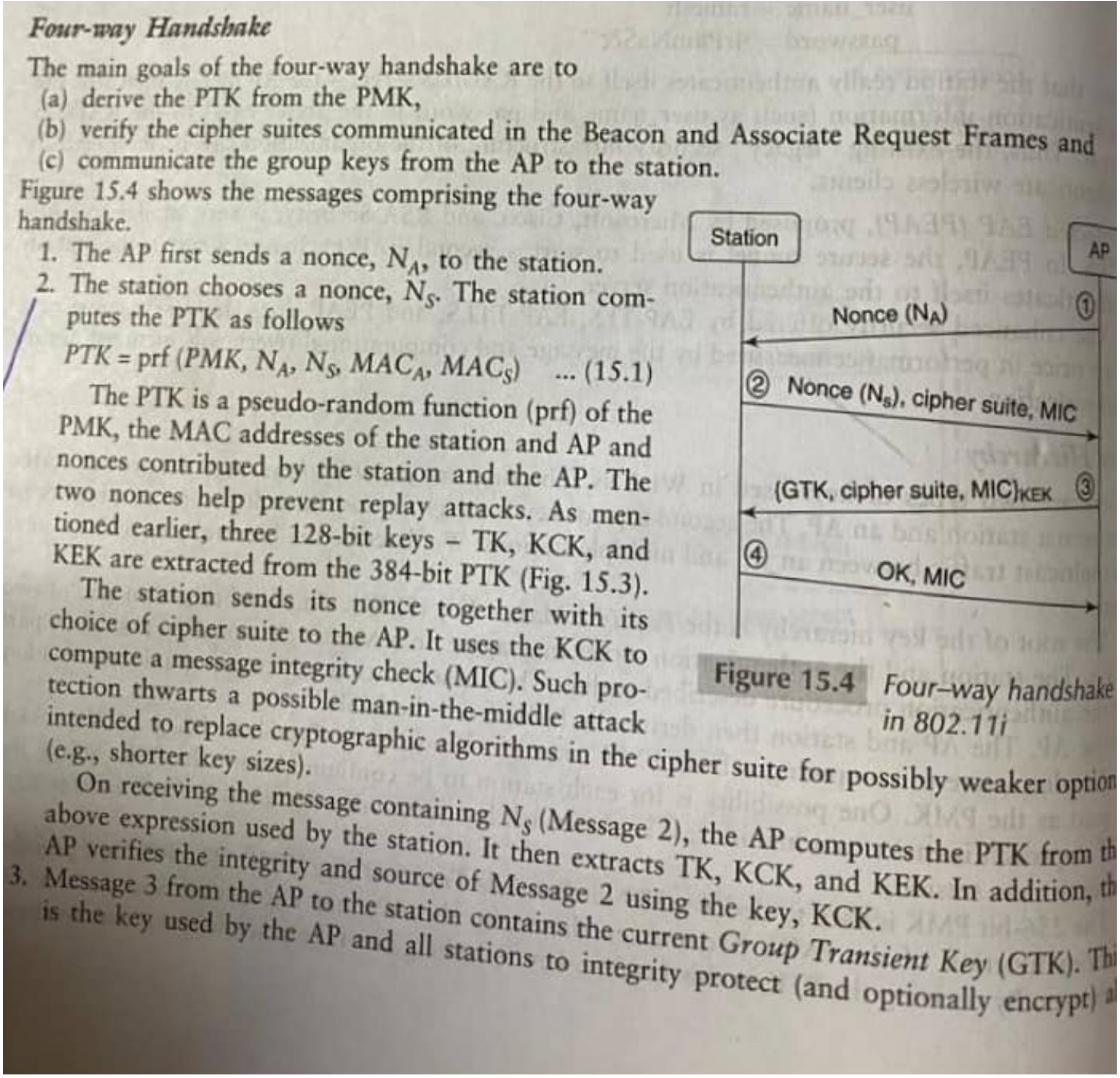
- Medusa is a command-line password cracking tool designed for network authentication-based services, such as SSH, FTP, Telnet, and various other protocols that require username/password authentication.
- It supports multiple authentication types, including basic authentication, NTLM, and more, making it versatile for cracking passwords used in different network services.
- Medusa is highly configurable, allowing users to specify parameters such as target hosts, usernames, passwords, and attack modes (e.g., dictionary, brute-force).

4. Hydra:

- Hydra is another command-line-based password cracking tool similar to Medusa but with a focus on network services like FTP, SSH, Telnet, HTTP(S), and more.
- It supports parallelized attacks, enabling simultaneous attempts against multiple targets or services, which can significantly speed up the password cracking process.
- Hydra is known for its flexibility and extensive protocol support, making it suitable for penetration testing and security assessments of network infrastructure and services.

It's important to note that while these tools can be valuable for legitimate security testing purposes, their misuse for unauthorized access to systems or accounts constitutes illegal activity and is strictly prohibited. Organizations should use these tools responsibly and within legal boundaries.

23. Explain Four way handshake in 802.11. CO2



Four-way Handshake

The main goals of the four-way handshake are to

(a) derive the PTK from the PMK,

(b) verify the cipher suites communicated in the Beacon and Associate Request Frames and

(c) communicate the group keys from the AP to the station.

Figure 15.4 shows the messages comprising the four-way handshake.

1. The AP first sends a nonce, N_A, to the station.
2. The station chooses a nonce, N_S. The station computes the PTK as follows

$$PTK = \text{prf}\,(PMK, N_A, N_S, MAC_A, MAC_S) \quad \ldots (15.1)$$

The PTK is a pseudo-random function (prf) of the PMK, the MAC addresses of the station and AP and nonces contributed by the station and the AP. The two nonces help prevent replay attacks. As mentioned earlier, three 128-bit keys – TK, KCK, and KEK are extracted from the 384-bit PTK (Fig. 15.3).

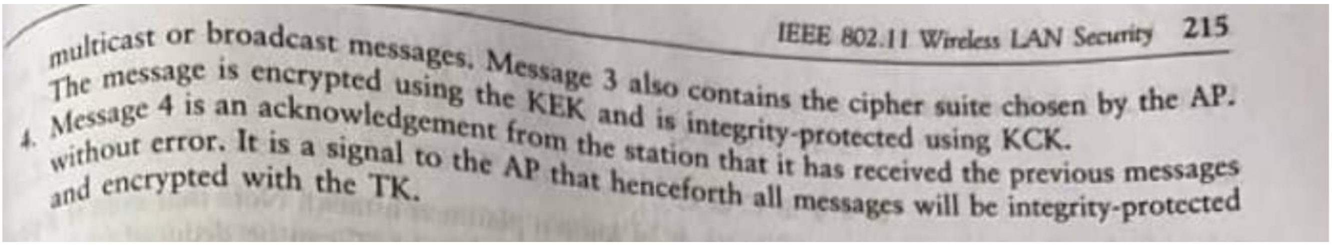
The station sends its nonce together with its choice of cipher suite to the AP. It uses the KCK to compute a message integrity check (MIC). Such protection thwarts a possible man-in-the-middle attack intended to replace cryptographic algorithms in the cipher suite for possibly weaker option (e.g., shorter key sizes).

On receiving the message containing N_S (Message 2), the AP computes the PTK from th above expression used by the station. It then extracts TK, KCK, and KEK. In addition, th AP verifies the integrity and source of Message 2 using the key, KCK.

3. Message 3 from the AP to the station contains the current *Group Transient Key* (GTK). Thi is the key used by the AP and all stations to integrity protect (and optionally encrypt) al

Station
AP
① Nonce (N_A)
② Nonce (N_S), cipher suite, MIC
(GTK, cipher suite, MIC)$_{KEK}$ ③
④ OK, MIC

Figure 15.4 *Four–way handshake in 802.11i*



IEEE 802.11 Wireless LAN Security 215

multicast or broadcast messages. Message 3 also contains the cipher suite chosen by the AP. The message is encrypted using the KEK and is integrity-protected using KCK.

4. Message 4 is an acknowledgement from the station that it has received the previous messages without error. It is a signal to the AP that henceforth all messages will be integrity-protected and encrypted with the TK.

24. Discuss how vulnerabilities in WEP were overcome in WPA Protocol. CO2

WEP, the Wired Equivalent Privacy protocol, was notoriously weak and susceptible to various attacks. WPA, or Wi-Fi Protected Access, was developed specifically to address these shortcomings and offer a more secure alternative. Here's how WPA tackled the vulnerabilities in WEP:

- Stronger Encryption: WEP relied on a static 40-bit key with a weak 24-bit initialization vector (IV). WPA introduced a more robust solution:
    - Larger key size: WPA uses a 256-bit dynamic key, significantly harder to crack than WEP's 40-bit key.
    - Temporal Key Integrity Protocol (TKIP): While WPA initially retained the RC4 encryption algorithm from WEP, it introduced TKIP. TKIP mixes the base key with a per-packet key, making it much more difficult to decrypt captured packets.
- Improved Integrity Checking: WEP's CRC-32 checksum was vulnerable to manipulation. WPA uses a stronger message integrity code (MIC) called Michael that detects any data tampering during transmission.
- Authentication: WEP lacked a proper authentication mechanism. WPA incorporated 802.1x Port-based Network Access Control (PNAC) for user authentication. This ensures only authorized devices can connect to the network.
- Key Management: WEP's static key was a major weakness. WPA uses a key hierarchy with a dynamically changing Temporal Key Integrity Protocol (TKIP) key and a master key managed by a centralized server. This makes it harder for attackers to exploit vulnerabilities in a single key.

While WPA was a significant improvement over WEP, it wasn't without its own limitations. WPA eventually led to the development of WPA2, which uses the stronger AES encryption algorithm and offers even more robust security features. WPA3, the latest iteration, further strengthens security with features like improved key management and stronger password hashing.

25. Explain plaintext attack in detail. CO2

There are two main types of plaintext attacks in cryptography, and the specific type determines the attacker's capabilities:

1. Known-Plaintext Attack (KPA):

In a known-plaintext attack, the attacker has access to both the original unencrypted message (plaintext) and its corresponding encrypted version (ciphertext). With this information, the attacker tries to crack the encryption system:

- Goal: The attacker's objective is to decipher the secret key or discover the encryption algorithm used. Once they have this knowledge, they can decrypt other messages encrypted with the same key.
- Example: Imagine a simple Caesar cipher where each letter is shifted a fixed number of positions. If an attacker intercepts a message containing "attack at dawn" along with its encrypted ciphertext, they can analyze the letter shifts between the plaintext and ciphertext to determine the key (number of positions shifted) and decrypt future messages.
- Classical Ciphers vs. Modern Cryptography: Known-plaintext attacks are particularly effective against older, weaker ciphers. Modern cryptographic algorithms are designed to be resistant to known-plaintext attacks, even with some plaintext-ciphertext pairs exposed.

2. Chosen-Plaintext Attack (CPA):

A chosen-plaintext attack grants the attacker a more powerful ability. Here, the attacker can select arbitrary plaintexts and get them encrypted by the target system. They then analyze the corresponding ciphertexts:

- Goal: Similar to a known-plaintext attack, the attacker aims to discover the secret key or encryption algorithm. However, the chosen-plaintext approach allows for a more systematic analysis by feeding the system with specific messages that might expose weaknesses.
- Challenges: Launching a chosen-plaintext attack may require some access or influence over the encryption system. This could involve compromising a part of the system that allows them to submit chosen plaintexts for encryption.
- Security in Modern Systems: Modern cryptographic systems are designed to be secure against chosen-plaintext attacks. This is achieved through techniques like randomizing ciphertexts to prevent patterns from leaking information about the key.

26. **Explain the working of TKIP and CCMP CO2**

TKIP (Temporal Key Integrity Protocol) and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) are encryption protocols used in Wi-Fi networks to secure data transmission.

TKIP (Temporal Key Integrity Protocol):
TKIP was developed as a temporary solution to improve the security of WEP (Wired Equivalent Privacy), which was found to be vulnerable to various attacks.
TKIP operates by dynamically changing encryption keys during the data transmission process. It uses a per-packet key mixing function to combine the original key with additional data, such as the packet sequence number and a unique transmitter address.
This dynamic key rotation mechanism helps mitigate certain types of attacks that exploit weaknesses in WEP, such as key reuse and statistical attacks.
However, TKIP still retains some of the vulnerabilities present in WEP and has been deprecated in favor of more secure encryption standards like CCMP.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):
CCMP is part of the IEEE 802.11i standard, also known as WPA2 (Wi-Fi Protected Access 2), which provides stronger security features compared to WEP and WPA (Wi-Fi Protected Access).
CCMP operates using the Advanced Encryption Standard (AES) algorithm in counter mode (CTR) for encryption and cipher block chaining (CBC) mode for message authentication.
It provides data confidentiality, integrity, and authentication by encrypting each data packet with a unique encryption key derived from a pairwise master key (PMK) established during the Wi-Fi authentication process.
CCMP uses a message authentication code (MAC) to ensure that data packets have not been tampered with during transmission.
Unlike TKIP, CCMP does not suffer from the vulnerabilities of WEP and offers stronger security, making it the recommended encryption protocol for modern Wi-Fi networks.

27. **Explain the working of our secret HOIC,XOIC,Burpsuite in brief(10-12 lines each)**

HOIC (High Orbit Ion Cannon): HOIC is a tool designed for conducting DDoS attacks. It allows users to flood target websites or servers with a high volume of traffic, causing them to become inaccessible to legitimate users. HOIC typically operates by coordinating a network of computers to simultaneously send traffic to the target, overwhelming its resources. It offers features like customizable attack parameters and the ability to join forces with other users for coordinated attacks.

XOIC (Xtreme Orbit Ion Cannon): Similar to HOIC, XOIC is a DDoS tool used for flooding target systems with traffic to disrupt their normal functioning. It enables users to launch large-scale attacks by leveraging multiple computers or devices to generate a massive volume of requests or data packets towards the target. XOIC provides various attack modes, including HTTP flooding and UDP flooding, allowing attackers to choose the most effective method for their objectives.

Burp Suite: Burp Suite is a comprehensive cybersecurity tool primarily used for web application security testing and penetration testing. It consists of several modules that facilitate various tasks such as scanning for vulnerabilities, intercepting and modifying web traffic, and analyzing the security of web applications. Burp Suite includes features like a proxy server for intercepting HTTP requests and responses, a scanner for automatically identifying common vulnerabilities, and tools for manual testing and exploitation. It is widely used by security professionals and ethical hackers to assess and improve the security posture of web applications.