ASSIGNMENT – 2

EXPLORING TOOLS OF KALI LINUX

1.WIRESHARK

Wireshark is a powerful network protocol analyzer that can be used to capture, analyze, and troubleshoot network traffic. It is a popular tool among network administrators, security professionals, and network engineers.

Here are some of the highlights of Wireshark:

- Comprehensive capture and analysis capabilities: Wireshark can capture and analyze traffic from a wide range of network protocols, including Ethernet, Wi-Fi, Bluetooth, and token ring. It can also capture traffic from encrypted connections.
- Powerful filtering and search capabilities: Wireshark allows you to filter and search captured traffic based on a variety of criteria, such as IP address, port number, and protocol type. This makes it easy to find specific packets or conversations of interest.
- Flexible display options: Wireshark can display captured traffic in a variety of formats, including text, hexadecimal, and packet summary. It also allows you to customize the display to your liking.
- Extensive documentation and support: Wireshark is well-documented and has a large and active community of users. This means that there is a wealth of information available to help you learn how to use Wireshark and troubleshoot problems.

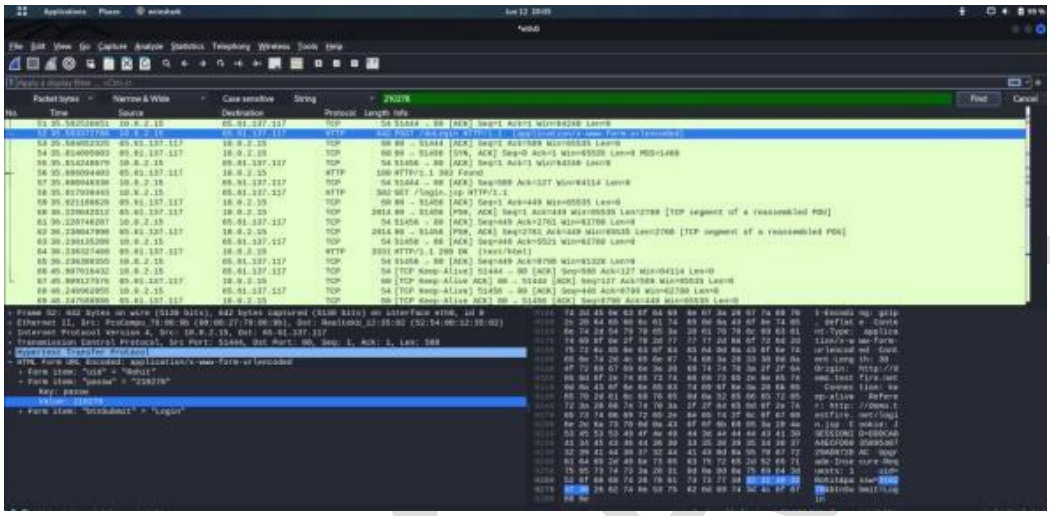
Wireshark is a free and open-source tool that is available for Windows, macOS, Linux, and Unix platforms. It is a powerful and versatile tool that can be used for a variety of purposes, including:

- Troubleshooting network problems: Wireshark can be used to troubleshoot network problems such as performance issues, connectivity issues, and security breaches.
- Analyzing network traffic: Wireshark can be used to analyze network traffic to understand how applications are using the network and to identify potential security threats.
- Learning about network protocols: Wireshark can be used to learn about network protocols by capturing and analyzing traffic from those protocols.

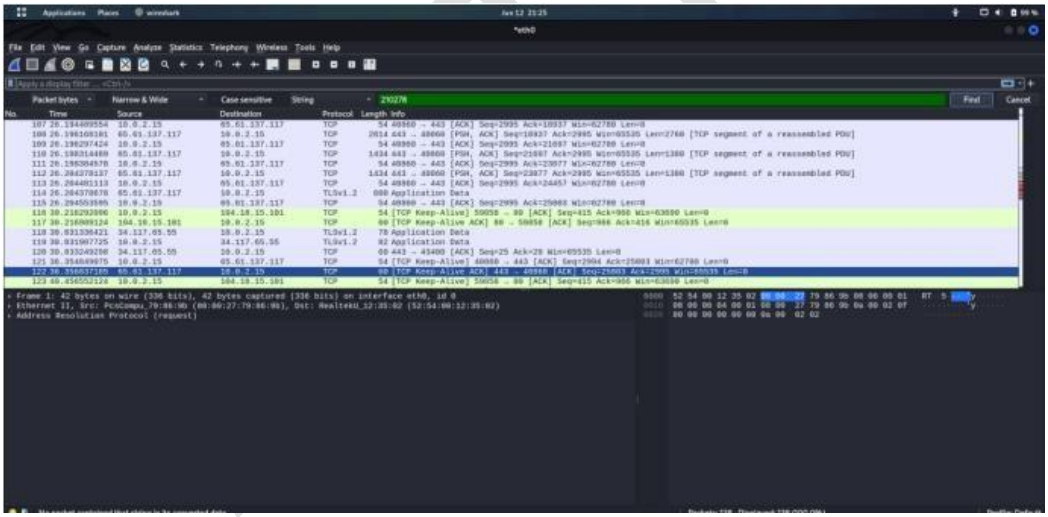
- Developing and testing network applications: Wireshark can be used to develop and test network applications by capturing and analyzing traffic from those applications.

Overall, Wireshark is a powerful and versatile network protocol analyzer that can be used for a variety of purposes. It is a free and open-source tool that is available for a variety of platforms.

A. FOR HTTP PROTOCOL -



B. FOR HTTPS PROTOCOL –



So wireshark works only for HTTP not for HTTPS protocol.

2. JOHN RIPPER –

John the Ripper is a free and open-source password cracking tool. It is one of the most popular and widely used password cracking tools in the world. John the Ripper is available for a variety of platforms, including Windows, macOS, Linux, and Unix.

John the Ripper can be used to crack passwords using a variety of methods, including brute-force attacks, dictionary attacks, and rule-based attacks. John the Ripper can also be used to crack passwords that are stored in a variety of formats, including encrypted passwords, hashed passwords, and shadow files.

John the Ripper is a powerful tool that can be used to crack passwords quickly and efficiently. However, it is important to note that John the Ripper is a dual-use tool. It can be used for both legitimate and malicious purposes. Legitimate uses of John the Ripper include security testing and password recovery. Malicious uses of John the Ripper include password cracking attacks and identity theft.

Here are some of the key features of John the Ripper:

- Supports a wide range of password cracking methods, including brute-force attacks, dictionary attacks, and rule-based attacks.
- Can crack passwords that are stored in a variety of formats, including encrypted passwords, hashed passwords, and shadow files.
- Highly customizable and extensible.
- Free and open source.

3. STEGHIDE TOOL –

Steghide is a steganography tool that can be used to hide data in image and audio files. It is a free and open-source tool that is available for Windows, macOS, and Linux. Steghide works by embedding the data to be hidden in the least significant bits of the image or audio file. This means that the hidden data is not visible to the naked eye and does not significantly affect the quality of the image or audio file.

Steghide can be used to hide a variety of data types, including text, images, and files. It can also be used to encrypt the hidden data to make it more difficult for unauthorized individuals to access.

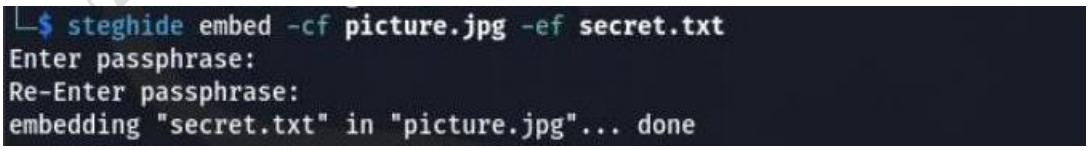
Steghide is a powerful tool that can be used for a variety of purposes, including:

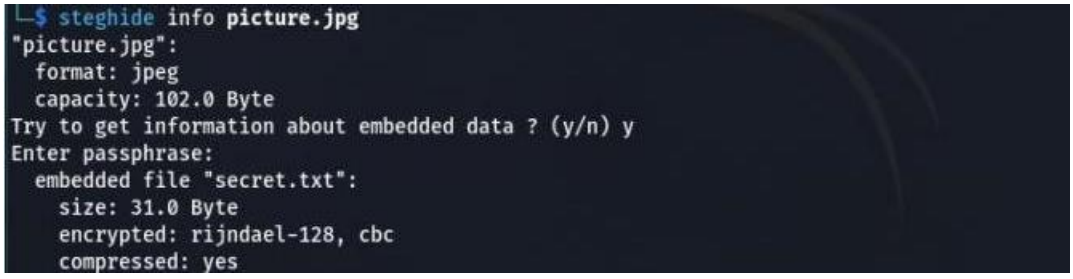
- Hiding sensitive data: Steghide can be used to hide sensitive data, such as passwords, financial information, and trade secrets, in image and audio files. This can help to protect the data from unauthorized access.
- Communicating secretly: Steghide can be used to communicate secretly by embedding messages in image and audio files. This can be useful for communicating in hostile environments or for bypassing censorship.
- Watermarking: Steghide can be used to watermark images and audio files. This can be used to prove ownership of the files or to deter unauthorized copying.

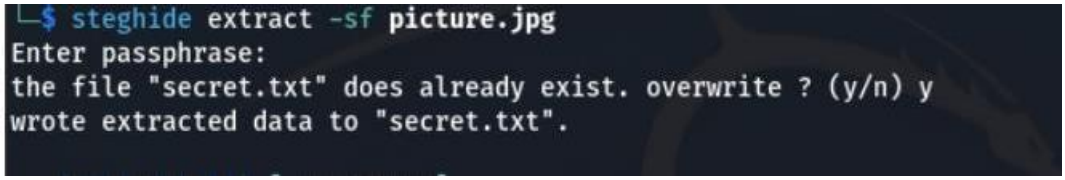
Steghide is a versatile tool that can be used for a variety of purposes. It is a popular tool among security professionals, journalists, and activists.

Here are some of the key features of Steghide:

- Supports embedding data in image and audio files
- Can encrypt hidden data
- Supports a variety of data types, including text, images, and files
- Is free and open-source
- Is available for Windows, macOS, and Linux







4. SOME MORE KALI TOOLS

Aircrack-ng: Aircrack-ng is a suite of tools for cracking WEP and WPA wireless passwords.

Nmap: Nmap is a network mapper that can be used to identify and map devices on a network.

~~**Wireshark:** Wireshark is a network protocol analyzer that can be used to capture and analyze network traffic.~~

Metasploit: Metasploit is a penetration testing framework that provides a wide range of tools for exploiting vulnerabilities and gaining access to systems.

Nessus: Nessus is a vulnerability scanner that can be used to identify vulnerabilities in systems and networks.

SQLMap: SQLMap is a tool for exploiting SQL injection vulnerabilities.

~~**John the Ripper**: John the Ripper is a password cracking tool.~~

Hydra: Hydra is a brute force attack tool that can be used to crack passwords, SSH keys, and other login credentials.

Maltego: Maltego is a tool for performing open-source intelligence (OSINT) gathering and analysis.

TheSleuthKit: TheSleuthKit is a toolkit for forensic investigations.

EnCase: EnCase is a commercial forensic toolkit.