**1- practical training**

**Topic:** Installing and configuring Wireshark

**The purpose of the work** is to provide students with the knowledge and skills to install and use the Wireshark application.Nazariy qism

The Wireshark application is a powerful network analyzer that can be used to analyze traffic passing through a computer's network interface. Performs the task of identifying and solving network problems, analyzing web applications, network programs or sites. Wireshark provides a complete view of the contents of packets at all levels.

Wireshark's development is driven by the efforts of network professionals around the world and is a continuation of a project started by Gerald Combs in 1998.

Wireshark works on most operating systems. Including Linux, Microsoft Windows, Solaris, FreeBSD, NetBSD, OpenBSD, Android and Mac OSX.

This application helps analyze data transmitted over hundreds of protocols.

These data packets can be analyzed in real-time or offline.

Wireshark has the following set of features:

* in-depth review of hundreds of protocols;
* online and offline analysis;
* standard three-panel package navigator;
* Works on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, etc.;
* received network data can be reviewed through GUI, TTY mode and TShark software;
* read / write many different file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN analyzer, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Networks Time Up Visual, WildPackets EtherPeek / TokenPeek / AiroPeek and more.
* online data can be read from Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, etc. (depending on the platform).
* Can be exported to XML, PostScript®, CSV or plain text.

**Practical part**

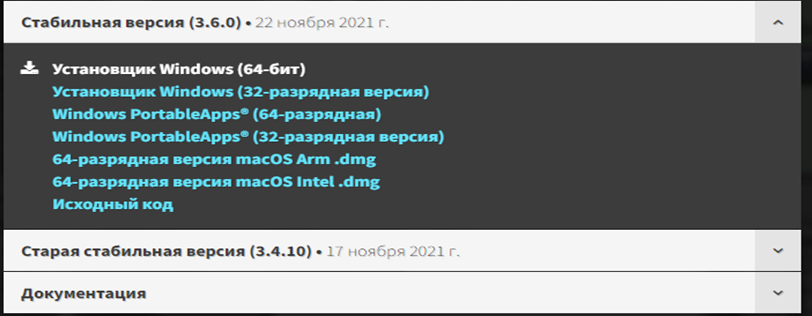
Before installing the Wireshark application, it is required to select the appropriate discharge application for the OS. This process is illustrated in Figure 1.1

Figure 1.1. OS charge selection window

In the next step, the sequence of configuring the selected application is performed.

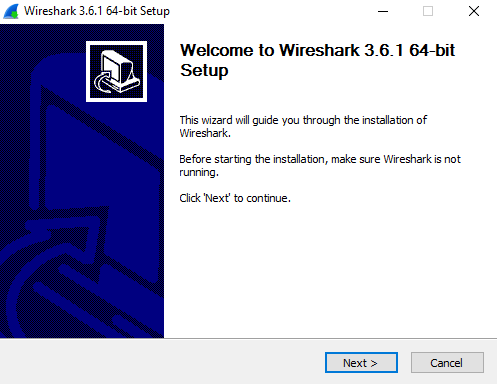


Figure 1.2. Application installation process

When configuring the Wireshark application, certain application parameters are also configured.

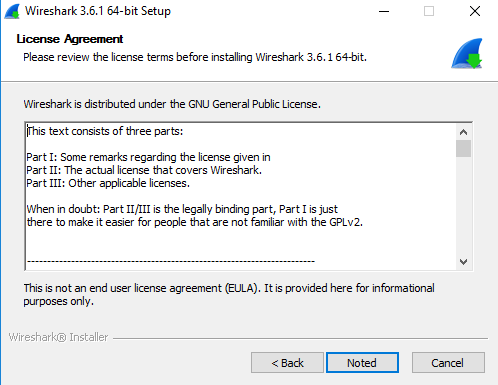


Figure 1.3. Consent to License

The process of installing additional applications from the Wireshark application is shown in the figure below.

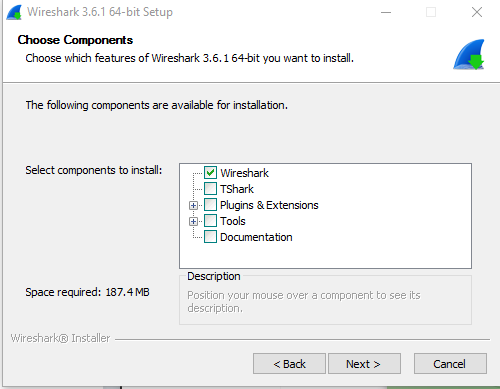


Figure 1.4. Add more tools

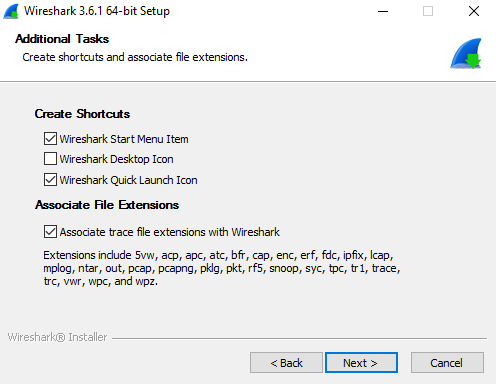
Additional tools also configure file extensions.

Figure 1.5. Set file extensions and shortcuts

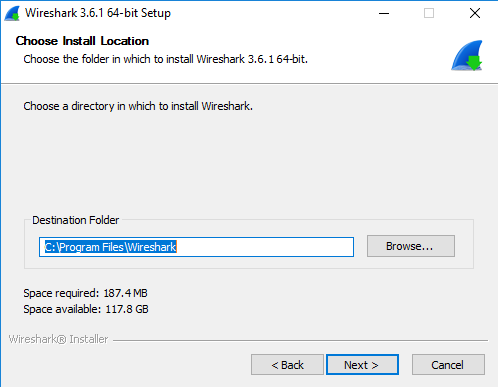
When configuring selected applications, space is required to store them.

Figure 1.6. Show where to install the app

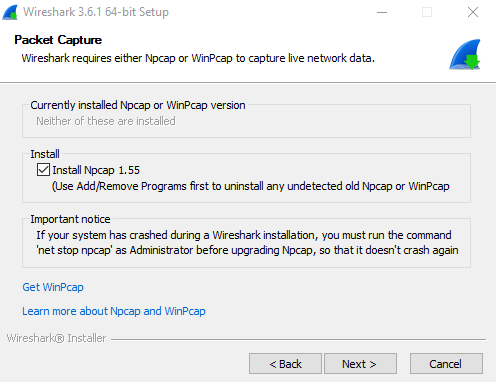
After the applications are configured, the traffic analysis tools are configured.

Figure 1.7. Install traffic analysis tools

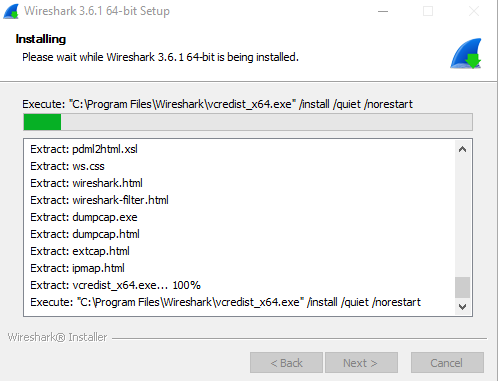
The "Npcap" section from the Wireshark application is also configured.

Figure 1.8. Npcap installation process

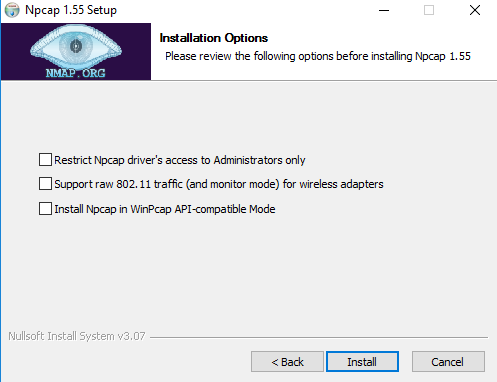
The Npcap installation process also defines its functions.

Figure 1.9. Npcap installation process

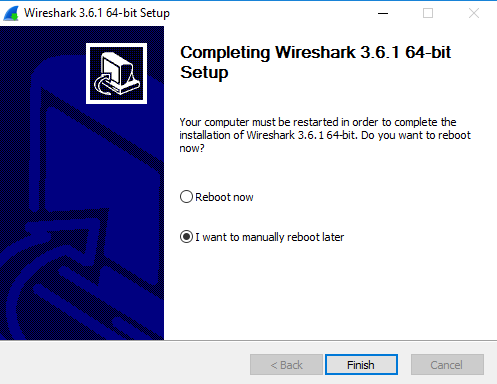
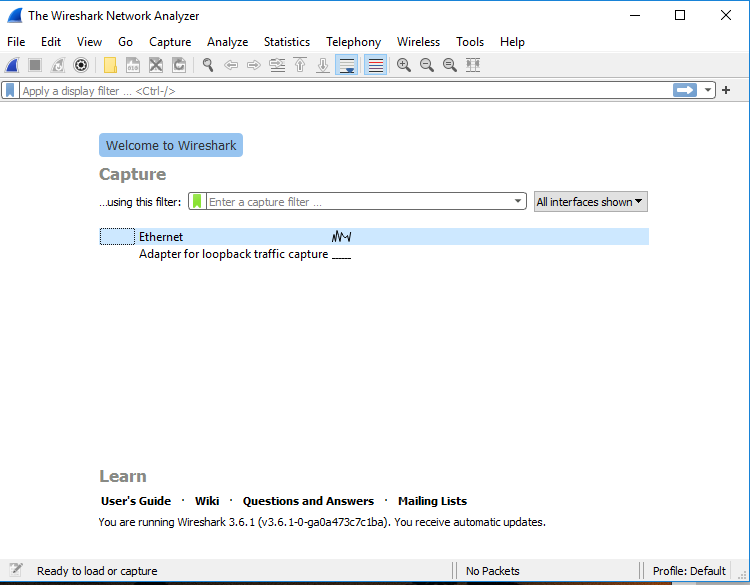
Npcap is configured after the above sequence.

Figure 1.10. Completing the npcap installation process

The image below shows the main window of the Wireshark application.

1.11- Working window of the Wireshark application

From the working window of the Wireshark application, you will be introduced to its configuration functions. The file part implements the saving of the parsed file and performs other tasks.

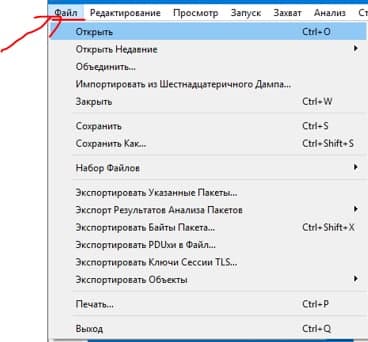
****

Figure 1.12. File window

In the "Editing" section, you can specify which part to go to, and write a comment on the packages.

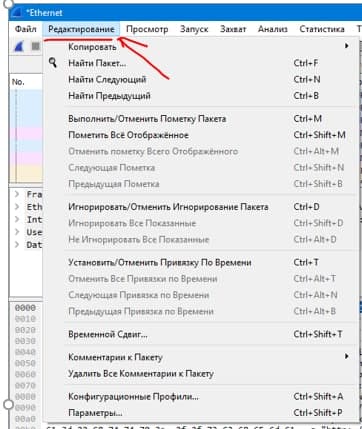


Figure 1.13. "Editing" window

We can separate the selected files into different sizes, view the program window in the general size and perform other tasks.

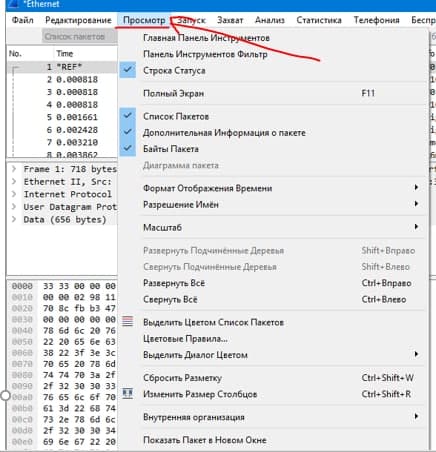


Figure 1.14. "Browse" window

In the "Zapusk" section, it transfers packets to the next part, the previous part, the first part, and the last part.

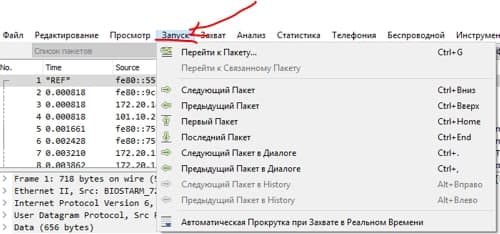


Figure 1.15. Zapusk window

In the "Zakhvat" part, it performs the tasks of turning on, turning off, and stopping the application.

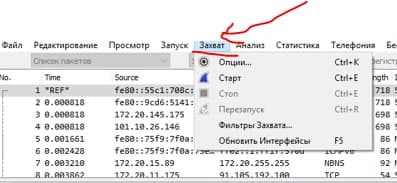


Figure 1.16. "Zakhvat" window

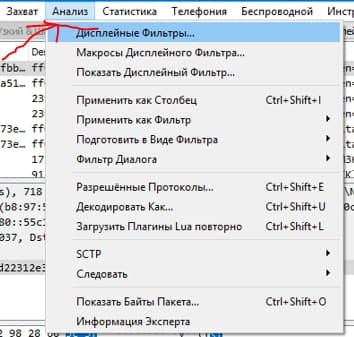
In the "Analysis" section, allowing protocols, filtering and other tasks are performed.

Figure 1.17. Analysis window

In the "Statistics" section, you can find out the characteristics of the files, the length of the package performs detection, DNS information and other tasks.

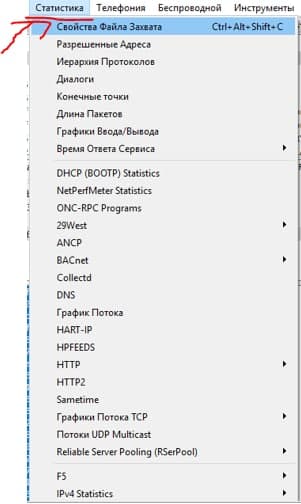


Figure 1.18. "Statistics" publication

In the "Telephony" section, you can analyze the ANSI, GMS network, view the packet count and perform other tasks.

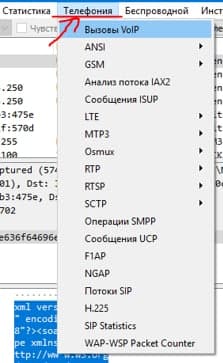


Figure 1.19. "Telephony" window

In the "Wireless" section, traffic analysis of the WLAN, selection of wireless technology usage, and other tasks are performed.

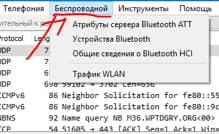


Figure 1.19. "Besprovodnoy" window

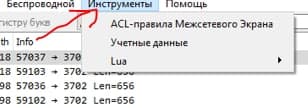
In the "Instrument" section, it performs other tasks such as viewing user information, getting acquainted with the rules of cross-network screens.

Figure 1.20. Instrument window

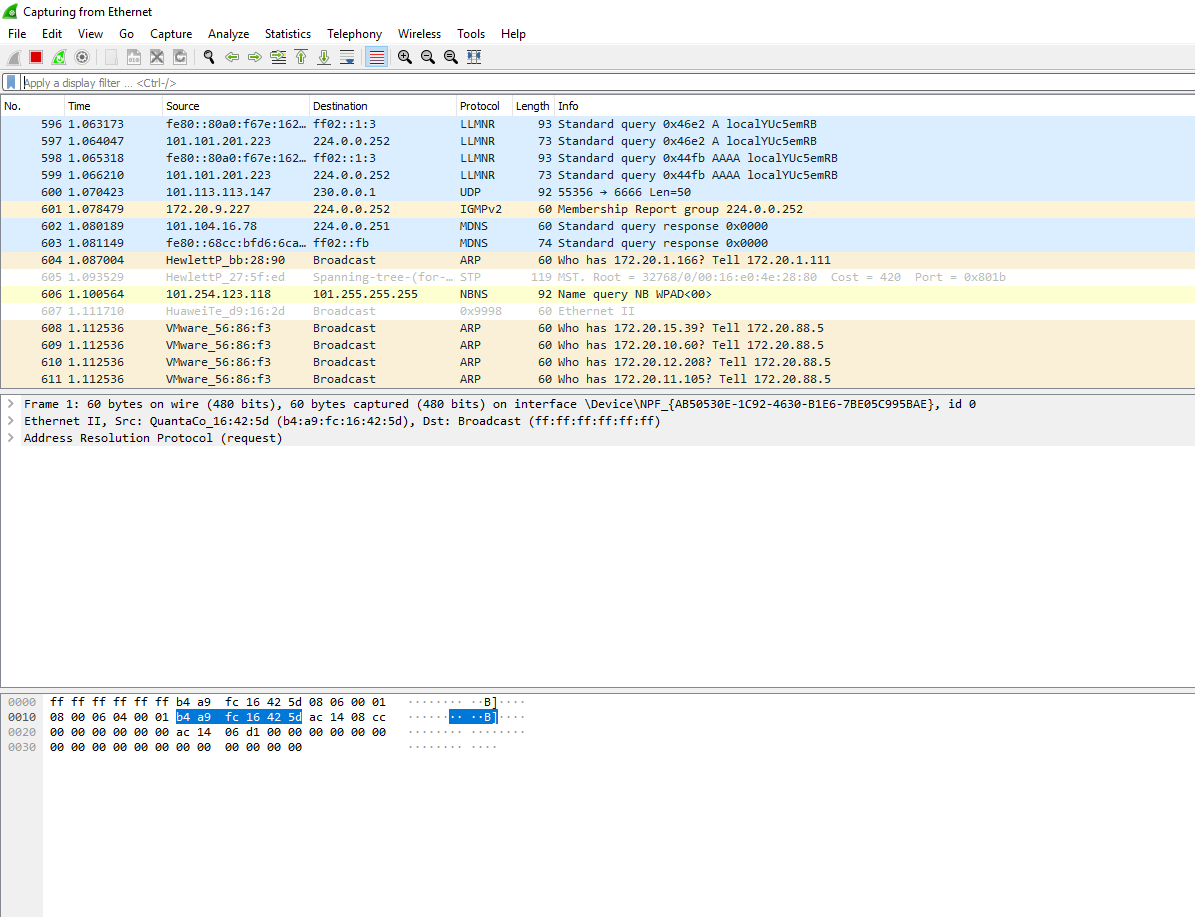
After using Wireshark with all its settings, we can analyze the network, for this we click on the blue start button and analyze it.

Figure 1.21. The result of the general network analysis

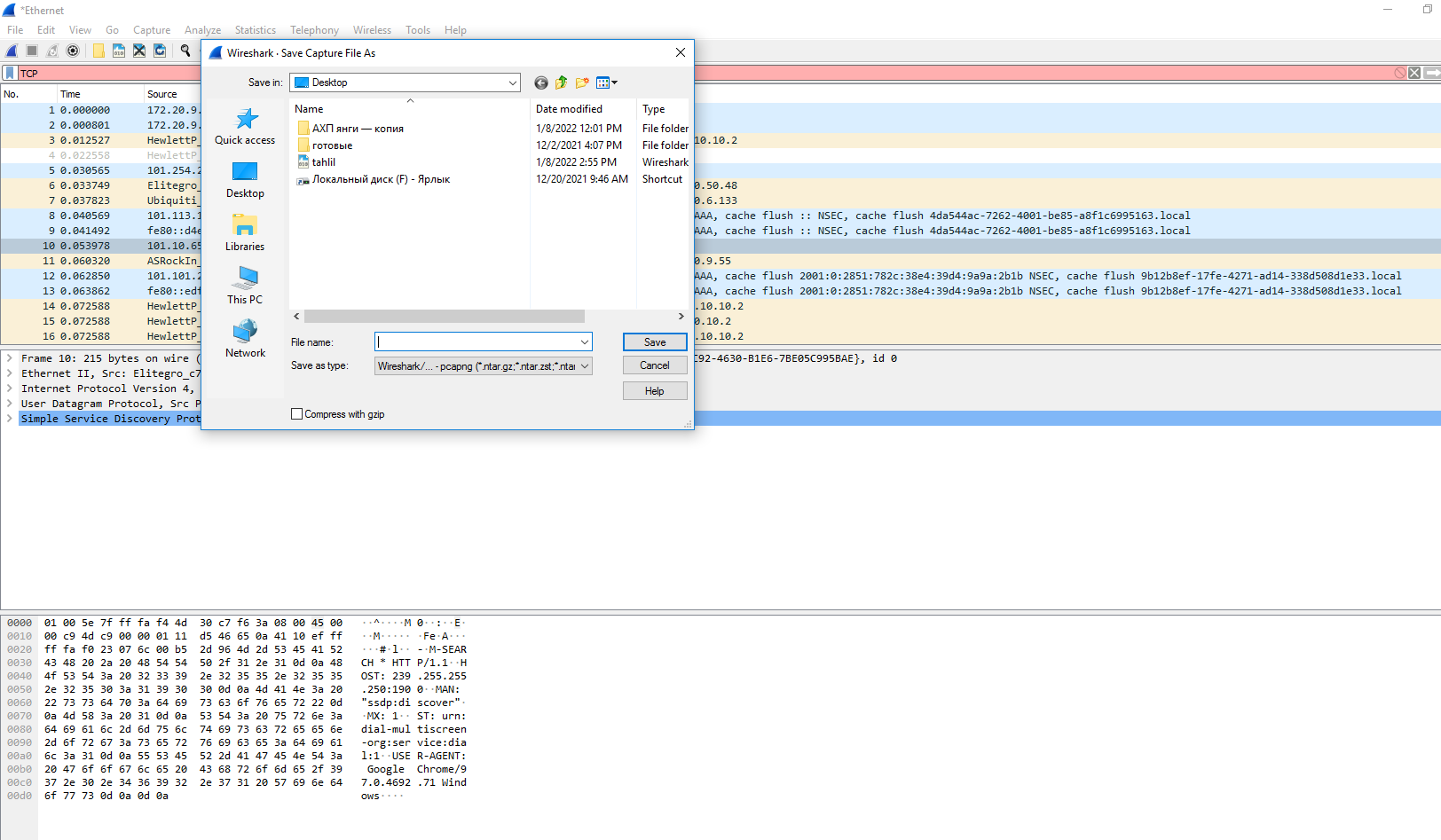
Based on the Wireshark application, the analyzed network can be cleaned.

Figure 1.21. Specifying the storage location of the general network analysis result

Assignment

Installing Wireshark on different OSes and familiarizing yourself with the toolbar.

**Control questions**

**1. What is the function of Wireshark?**

**2. What should be considered when choosing the Wireshark program?**

**3. What is the feature set of the Wireshark application?Foydalanilgan adabiyaotlar**

1. <https://www.wireshark.org/#download (murojat> vaqti: 20.12.21)
2. [https://www.wireshark.org/docs//wsug\_html\_chunked/ChIOSaveSection.ht](https://www.wireshark.org/docs/wsug_html_chunked/ChIOSaveSection.ht)
3. <https://www.wireshark.org/download.html>
4. <https://www.wireshark.org/#download (murojat> vaqti: 20.12.21)