Learning diary and answers

These are optional fields about your identity, leave empty if you want to remain anonymous:

Student name: Ashif Ahmed Khan Moon

Email address (prefer your @students.oamk.fi email if you have such address):
t2moas00@students.oamk.fi

Save the final version of this document as PDF and submit it for peer reviews via Moodle's workshop tool before the deadline. Last course week is for peer reviews.

Some courses may have 5 weeks, and some may have 8 weeks of assignments. This is a generic learning diary template. Adapt and edit the document accordingly.

Week 1

Question 1: Define following terms and concepts shortly:

- Network bandwidth
- Network throughput
- Packet loss and jitter
- bps vs Bps
- Protocol payload
- Protocol overhead (especially for resource-contrained IoT purposes)
- Spanning Tree Protocol
- Collision domain
- Broadcast domain
- SOHO network
- MAC (physical) address
- Physical layer protocol data unit (PDU)
- MAC layer protocol data unit (PDU)
- Half-duplex vs Full-duplex
- Ethernet auto-negotiation
- Hidden node problem (wireless)
- Networking physical vs logical topology
- TIA/EIA-568 and ISO/IEC_11801
- Ethernet cabling categories. For example, CAT 6
- 8P8C (RJ45)
- Wifi AD HOC
- IEEE 802.11ac, 802.11ax, 802.11be

Answer 1: Definition of the following terms are given below :

Network Bandwidth: The maximum data transfer rate of a network, typically measured in bits per second (bps), indicating the capacity of the connection.

Network Throughput: The actual amount of data successfully transferred over a network in a given time period, often less than the bandwidth due to various inefficiencies.
Packet Loss: The percentage of data packets that are sent but not received, often leading to reduced network performance.

Jitter: The variation in packet arrival times, leading to disruptions in applications like voice and video streaming.

bps (bits per second): A measure of data transfer speed in bits.
Bps (Bytes per second): A measure of data transfer speed in bytes (1 byte = 8 bits).

Protocol Payload: The actual data being carried in a network message, excluding the headers.

Protocol Overhead: Extra data added to the protocol's payload for managing the transmission, which is crucial to minimize in resource-limited devices like IoT.

Spanning Tree Protocol (STP): A protocol that prevents network loops by creating a tree structure that disables redundant paths in Ethernet networks.

Collision Domain: A network area where data packets can collide with each other if sent simultaneously, causing delays.

Broadcast Domain: A network area where any broadcast message is received by all devices.

SOHO Network: Small Office/Home Office network; a simple, low-cost network setup for small spaces.

MAC (Physical) Address: A unique identifier assigned to network devices for communication on a local network.

Physical Layer Protocol Data Unit (PDU): The data format used at the physical layer of networking, typically consisting of raw bits.

MAC Layer Protocol Data Unit (PDU): The data format at the MAC layer, often a frame with a header and data.

Half-Duplex: Communication in one direction at a time.
Full-Duplex: Communication in both directions simultaneously

Ethernet Auto-Negotiation: A feature that allows Ethernet devices to automatically choose the best speed and mode for communication.

Hidden Node Problem (Wireless): A situation where a device can communicate with an access point but not with other devices, leading to possible data collisions.

Physical Topology: The actual layout of devices and cables in a network.
Logical Topology: The way data flows through the network, regardless of physical layout.

TIA/EIA-568 and ISO/IEC 11801: Standards for network cabling that ensure reliable performance by specifying installation and testing methods.

Ethernet Cabling Categories: Different types of Ethernet cables, with categories like CAT 5e, CAT 6, indicating performance levels and speed capabilities.

8P8C (RJ45): A type of connector commonly used in Ethernet networks, with 8 positions and 8 contacts.

WiFi AD HOC: A wireless network configuration where devices connect directly to each other without a central access point.

802.11ac: A WiFi standard for high-speed wireless connections in the 5 GHz band.

802.11ax (WiFi 6): An improved WiFi standard that increases speed and efficiency in both 2.4 GHz and 5 GHz bands.

802.11be (WiFi 7): The upcoming WiFi standard designed to provide even faster and more efficient wireless connections.

Question 2: Estimate how long does it take to download 3 TB file from cloud based backup service if network download throughput is 200 Mbps for actual payload (i.e. data)?

Answer 2: to estimate the time first we have to convert the file size to bits then we have to calculate the total file size in bits after that we have to convert the download speed in bits per second then we will estimate the time required and finally convert the seconds to hours.

So, 3 TB = 25769,803,776,000 bits
200Mbps = 200,000,000 bits per second.
Now the download time= 25769,803,776,000 bits / 200,000,000 bits per second.
=128,849.02 seconds
Then the time in hours =128,849.02 seconds /3600 seconds per hour =35.79 hours.

So it would take around 35.79 hours.

Question 3: Locate the MAC address of your mobile phone, laptop wifi interface or some other networked IT device

- How did you find it?
- List the MAC address in hex format (such as f0:1f:af:cf:d9:1a), but replace last 24 bits with zeros for your privacy
- Use OUI MAC address list(s) or lookup tools, and determine the device/chipset vendor of that MAC address. For example, that f0:1f:af:cf:d9:1a is Dell inc.

Answer 3:As I use a mac book to found my mac address I went to system preference then went to network option then I clicked on wifi details after that hardware option.
My mac addreass is c4:35:d9:00:00:00

Question 4: Describe shortly what are these network devices, functions, and services

- Repeater
- Hub (multiport repeater)
- Bridge
- Access switch
- Core switch
- Edge router
- Core router
- Firewall
- Wifi AP
- WLAN AP controller
- Network TAP

Answer 4:Short description of above terms are given below:-

Repeater: Amplifies or regenerates network signals to extend the distance they can travel.Used to boost weak signals in a network, often in long cable runs or wireless networks.

Hub (Multiport Repeater): Connects multiple network devices, broadcasting data to all connected devices. Operates at the physical layer (Layer 1) and is typically used in simple networks. It can cause network congestion since it sends data to all ports.

Bridge: Connects and filters traffic between two or more network segments, reducing collisions.Operates at the data link layer (Layer 2), learning MAC addresses to forward data only to the correct segment.

Access Switch: Connects end devices like computers and phones to the network. Operates at Layer 2, forwarding data within the local area network (LAN) and providing basic network management features.

Core Switch:High-performance switch that connects multiple access switches and manages data traffic within the backbone of the network.Operates at Layers 2 and 3, handling large amounts of traffic and routing data across different parts of a network.

Edge Router:Routes data between one or more local networks and external networks, such as the internet.Operates at Layer 3, managing traffic to and from external sources and often handling network address translation (NAT) and security functions.

Core Router:High-capacity router that directs data within a large, high-speed backbone network.Operates at Layer 3, efficiently managing large-scale data routing within a core or backbone network, often between data centers.

Firewall:Monitors and controls incoming and outgoing network traffic based on security rules. Provides security by filtering traffic, preventing unauthorized access, and blocking malicious traffic.

WiFi Access Point (AP):Allows wireless devices to connect to a wired network using WiFi.Extends the range of a wireless network and enables wireless devices to communicate with the network.

WLAN AP Controller:Manages multiple WiFi access points, providing centralized configuration, monitoring, and control. Simplifies the management of large wireless networks, ensuring consistent configuration and performance across all APs.

Network TAP (Test Access Point):Passively captures and monitors network traffic for analysis without disrupting the network.Used for network monitoring, troubleshooting, and security analysis by providing a copy of the network traffic to monitoring devices.

Question 5: RFC assignments

- What are RFCs?
- How many PPP related RFC documents can you find from rfc-editor website?
- What is the current status of RFC1597? What is the number for updated, more recent RFC of same topic?
- When was RFC5218 released?
- What is the meaning if RFC status is BCP?
- List authors of the CoAP RFC (June 2014). What is the RFC number?
- Twitch.tv provides IRC access to the stream chats. Which RFC defines the original Internet Relay Chat (IRC) Protocol?

Answer 5: RFCs (Request for Comments) are documents published by the Internet Engineering Task Force (IETF) and other working groups that describe the specifications, protocols, procedures, and policies related to the internet and networking technologies. RFCs can serve as official standards, informational documents, or experimental protocols.

I have found 216 documents from rfc editor website on point to point protocol.

RFC 1597 which defines private IP address ranges currently has historic status the most recent RFC that updates RFC 1597 is RFC 1918.

RFC 5218 was released in July 2008.

BCP stands for Best Current Practice. When an RFC has a BCP status, it indicates that the document contains recommendations or practices that are currently considered the best approach to a certain issue or procedure in internet protocols and technologies.

Authors of CoAP RFC is Zach Shelby,Klaus Hartke, Carsten Bormann.The RFC number is RFC 7252.

RFC 1459 defines the internet Relay Chat protocol.

Question 6: What is OSI model? Compare OSI model to TCP/IP model?

Answer 6: The Open Systems Interconnection (OSI) model is a conceptual framework that divides network communications functions into seven layers. Sending data over a network is complex because various hardware and software technologies must work cohesively across geographical and political boundaries. The OSI data model provides a universal language for computer networking, so diverse technologies can communicate using standard protocols or rules of communication. Every technology in a specific layer must provide certain capabilities and perform specific functions to be useful in networking. Technologies in the higher layers benefit from abstraction as they can use lower-level technologies without having to worry about underlying implementation details.

Comparison between OSI and TCP/IP :-

The OSI (Open Systems Interconnection) Model and the TCP/IP (Transmission Control Protocol/Internet Protocol) Model are two frameworks used to understand how data moves through networks. While they both help in organizing network communication, they have distinct structures and purposes. Understanding these differences is essential for anyone learning about or working with computer networks. while both the OSI Model and TCP/IP Model are essential for understanding network communication, they differ in their structure and practical application. The OSI Model provides a theoretical framework with seven layers, emphasizing clear separation of functions, while the TCP/IP with its four layers, reflects the protocols used on the internet today. Each model offers unique insights into how data is transmitted across networks, catering to different aspects of network design, management, and troubleshooting.

Week 2

Question 7: What are VLANs and IEEE 802.1q?

Answer 7 :
VLANs (Virtual Local Area Networks): A VLAN is a logical partition of a physical network. It allows you to group devices on a network into segments, regardless of their physical location. VLANs are used to enhance network performance and security.

IEEE 802.1Q is a standard for implementing VLANs in Ethernet networks. It specifies how to tag Ethernet frames so that they can be identified as belonging to a particular VLAN.

VLANs allow for logical segmentation of a network, while IEEE 802.1Q is the standard that enables VLANs to be effectively implemented on Ethernet networks by tagging frames with VLAN identifiers.

Question 8:Define following terms and concepts shortly:

- ARP
- ARP spoofing
- HOP (networking)
- IP TTL
- IP TOS (DSCP)
- DHCP, DHCP relay
- WoL (Wake-on-LAN)
- UPnP
- Traceroute / Tracepath
- Network Address Translation (NAT)
- Tier 1 and 2 networks
- Tier 3 ISP
- Routing Autonomous System (AS or ASN for BGP)
- 127.0.0.1 address
- ::1 address
- 0.0.0.0/0 and ::/0 networks in the routing table
- Ranges of IPv4 multicast and experimental addresses

Answer 8:Short description of above terms are given below=

Certainly! Here's a concise explanation of each term and concept:

ARP (Address Resolution Protocol):A protocol used to map an IP address to a MAC address in a local network.
ARP Spoofing:A type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device, potentially intercepting or altering traffic.
HOP (Networking):A hop refers to the journey of a packet between two network devices or routers in a network path.

IP TTL (Time to Live):A field in an IP packet that indicates the maximum number of hops (routers) the packet is allowed to pass through before being discarded. It helps prevent packets from circulating indefinitely.

IP TOS (Type of Service) / DSCP (Differentiated Services Code Point):
TOS is an older IP field for specifying the priority of a packet; DSCP is its modern replacement, used to classify and manage network traffic for quality of service (QoS).

DHCP (Dynamic Host Configuration Protocol):A network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network.

DHCP Relay:A method used to forward DHCP messages between clients and servers that are not on the same local network segment.

WoL (Wake-on-LAN):A feature that allows a networked computer to be turned on or woken up from a low power state remotely via a network message.

UPnP (Universal Plug and Play):A set of networking protocols that allows devices to discover each other and establish functional network services automatically.

Traceroute / Tracepath:Tools used to trace the route packets take from one host to another, showing each hop along the path and the time taken.
Network Address Translation (NAT):A technique used to modify network address information in IP packet headers while in transit across a routing device, commonly used to allow multiple devices on a private network to share a single public IP address.

Tier 1 and 2 Networks:
-Tier 1 Network: Large ISPs with extensive networks that exchange traffic with each other without charge.
- Tier 2 Network: ISPs that purchase transit from Tier 1 ISPs or other Tier 2 ISPs to provide broader internet access.

Tier 3 ISP:
ISPs that primarily resell bandwidth from Tier 1 or Tier 2 ISPs to end customers and do not have extensive networks of their own.

Routing Autonomous System (AS or ASN for BGP):
A collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet. ASN (Autonomous System Number) is a unique number assigned to each AS for identification in BGP routing.

127.0.0.1 Address:The loopback address in IPv4, used by a device to refer to itself for testing and communication within the same device.

::1 Address:The loopback address in IPv6, serving the same purpose as 127.0.0.1 in IPv4.

0.0.0.0/0 and ::/0 Networks in the Routing Table:
- 0.0.0.0/0: Represents the default route in IPv4, meaning all IP addresses.
- ::/0: Represents the default route in IPv6, covering all possible IPv6 addresses.

Ranges of IPv4 Multicast and Experimental Addresses
- IPv4 Multicast Addresses: 224.0.0.0 to 239.255.255.255
- IPv4 Experimental Addresses: 240.0.0.0 to 255.255.255.255 (generally reserved for experimental use and not used in regular internet communication)

Question 9: Search some information about AS1741

- Which organisation or company advertises AS1741 with BGP?
- List some public peering exchange points the AS1741 connects to?
- To which regional internet registry (RIR) the AS1741 belongs to?
- What is the contact email address/phone/web form if you would need to inform some security or abuse issues to the owner of the AS1741?

Answer 9:
AS1741 is advertised by AOL Inc. (America Online). This AS number is associated with their network for routing and connectivity purposes.
AS1741 (AOL Inc.) is known to connect to several public peering exchange points. Some notable ones include:

1. Equinix IX (various locations, including Ashburn, DC and Dallas, TX)
2. DE-CIX (Frankfurt, Germany)
3. LINX (London Internet Exchange, London, UK)

These exchange points facilitate the exchange of traffic between networks and can provide redundancy and improved performance. The exact peering points can vary over time.
AS1741 is registered with ARIN (American Registry for Internet Numbers). ARIN is the Regional Internet Registry (RIR) responsible for managing IP address space and Autonomous System Numbers (ASNs) in North America.

For security or abuse issues related to AS1741 (AOL Inc.), you can use the following contact information:Email: abuse@aol.com.
They don't publicly advertise there phone number specifically for abuse email is the primary contract method.But for recent update anyone can check AOL's Support or contact page.

Question 10: What it the difference between static and dynamic routing? Use example(s)
Answer 10:
Static routing and dynamic routing are two primary methods used to determine the best path for data packets to travel through a network. The key difference lies in how the routing decisions are made.
Static Routing:-
In static routing, the network administrator manually configures the routes between network devices. These routes remain fixed unless the administrator manually changes them.
Example: Imagine a small network with three routers (A, B, and C). The administrator manually configures router A to send packets destined for network C through router B. If the link between routers B and C fails, packets from router A will continue to be sent through router B, even though it's no longer reachable.
Advantages:

- Predictability: Routes are known and consistent, ensuring predictable network behavior.
- Simplicity: Configuration is straightforward, especially in small networks.
- Security: Can be used to restrict traffic flow and improve security.

Disadvantages:

- Manual configuration: Requires constant monitoring and manual updates.
- Inefficiency: Routes may not always be optimal, leading to inefficient use of network resources.
- Lack of adaptability: Cannot adapt to changes in network topology or traffic patterns.

Dynamic Routing:-
In dynamic routing, routers automatically learn about network topology and traffic conditions. They use routing protocols to exchange information with other routers and dynamically adjust routes to optimize data flow.
Example: Using the same network as before, routers A, B, and C would use a dynamic routing protocol (e.g., OSPF, RIP) to exchange information about their connected networks. If the link between routers B and C fails, the routers will automatically re-calculate routes and find alternative paths for packets.
Advantages:

- Adaptability: Routes are automatically adjusted to changes in network conditions.
- Efficiency: Routes are typically more optimal, improving network performance.
- Scalability: Well-suited for large networks with complex topologies.

Disadvantages:

- Complexity: Configuration can be more complex, especially in large networks.
- Convergence time: It may take time for routers to converge on new routes after a topology change.

- Security risks: Dynamic routing protocols can be susceptible to security threats like routing table poisoning.

In summary, static routing is suitable for small, stable networks where manual configuration is feasible. Dynamic routing is better suited for larger, more dynamic networks that require automatic route adjustments to optimize performance and adapt to changes.

Question 11:Describe briefly these dynamic routing protocols

- RIP
- OSPF and IS-IS
- BGP
- RPL (ripple)

Answer 11: Dynamic Routing Protocols :

RIP (Routing Information Protocol):

- A distance-vector routing protocol that uses hop count as a metric to determine the shortest path.
- Each router broadcasts its routing table to its neighbors periodically.
- Simple to implement but can suffer from slow convergence and routing loops.
- Best suited for small networks with stable topologies.

OSPF (Open Shortest Path First):

- A link-state routing protocol that calculates the shortest path using Dijkstra's algorithm.
- Each router maintains a map of its network topology and shares this information with its neighbors.
- Offers faster convergence and is more resistant to routing loops than RIP.
- Well-suited for large networks with complex topologies and high traffic volumes.

IS-IS (Intermediate System to Intermediate System):

- Similar to OSPF but designed specifically for intermediate systems in networks like ATM and Frame Relay.
- Uses a hierarchical topology to scale efficiently in large networks.
- Offers similar advantages to OSPF in terms of convergence speed and routing loop prevention.

BGP (Border Gateway Protocol):

- A policy-based routing protocol used to interconnect different autonomous systems (ASes).
- Routers exchange routing information using a path attribute system that allows for fine-grained control over routing decisions.
- Supports various routing policies, including path length, policy-based routing, and route filtering.
- Essential for the interconnection of large-scale networks and the internet.

RPL (Routing Protocol for Low-Power and Lossy Networks):

- Designed specifically for IoT networks with limited resources and unreliable links.
- Uses a hierarchical topology and a parent-child relationship between nodes to conserve energy and improve reliability.
- Offers features like objective function, route optimization, and data forwarding mechanisms.
- Well-suited for applications like smart homes, sensor networks, and industrial IoT.

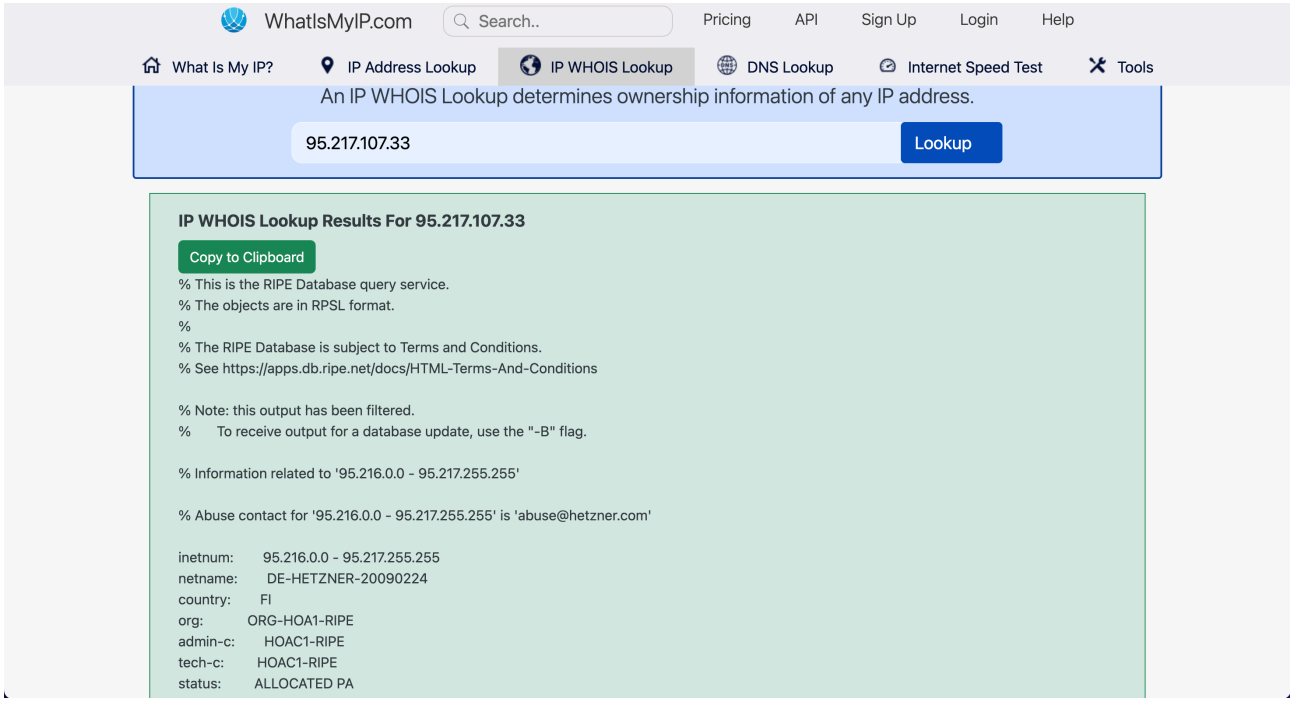
By understanding the characteristics and capabilities of these dynamic routing protocols, network administrators can select the most appropriate protocol for their specific network requirements and ensure efficient and reliable data transmission.

Question 12. Create a DNS request (any tool such as ping, nslookup, whatever) to resolve the IP address of www.oamk.fi

- Use some IP whois lookup web service to resolve which company is hosting and has that IP address and server? (www.oamk.fi)
- What is the inetnum or route/network (IP address range) the www.oamk.fi's IP address belongs to?
- What is abuse contact email address of that network range?

Answer 12:

```
ashifmoon@Ashifs-MacBook-Air ~ % ping www.oamk.fi
PING fi-haarla.seravo.com (95.217.107.33): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
Request timeout for icmp_seq 15
Request timeout for icmp_seq 16
Request timeout for icmp_seq 17
Request timeout for icmp_seq 18
Request timeout for icmp_seq 19
Request timeout for icmp_seq 20
```



For any reports related to abuse or malicious activity originating from this IP range, the designated abuse contact email is abuse@upcloud.com(IP Tracker). This is the standard contact for handling network abuse issues for servers hosted by UpCloud, including cases such as spam, hacking attempts, or other forms of misuse.

Question 13: Use traceroute (tracert in MS Windows command shell) to www.whitehouse.gov

- What is the internet service provider's first router IP address near you? (it's most likely the 2nd router/hop, immediately after your home network)
- How many hops (routers) are there to the www.whitehouse.gov from your device?
- Use traceroute again, but this time to Google's public DNS server in 8.8.8.8, and Quad9 DNS in 9.9.9.9. How far are those?
- Why traceroute does not always work, and does not show the route up to the final destination IP, or there are timeouts for some routers (* is timeout)? For example, IP address of education.gov.au
- Use traceroute and DNS to estimate/guess from response DNS names, round trip times, and with IP whois lookups, where the web server reliefweb.int is located (continent, country or so)?

Answer 13:

```
Last login: Sun Sep 15 09:28:31 on ttys000
[ashifmoon@Ashifs-MacBook-Air ~ % traceroute www.whitehouse.gov                  ]
traceroute to wh46.go-vip.net (192.0.66.168), 64 hops max, 40 byte packets
 1  172.20.10.1 (172.20.10.1)  4.703 ms  4.267 ms  4.691 ms
 2  * * *
 3  * * *
 4  193.229.29.197 (193.229.29.197)  64.223 ms  27.359 ms  33.022 ms
 5  213.192.184.80 (213.192.184.80)  60.905 ms  26.874 ms  27.078 ms
 6  213.192.184.93 (213.192.184.93)  32.892 ms  38.836 ms  43.853 ms
 7  netnod-ix-ge-a-sth-1500.automattic.com (194.68.123.63)  57.917 ms  47.042 ms
  58.794 ms
 8  * *
```

```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  172.20.10.1 (172.20.10.1)  6.977 ms  3.532 ms  3.292 ms
 2  * * *
 3  * * *
 4  193.229.29.197 (193.229.29.197)  67.239 ms  27.824 ms  28.755 ms
 5  213.192.184.80 (213.192.184.80)  34.855 ms  27.615 ms  27.957 ms
 6  213.192.184.177 (213.192.184.177)  31.722 ms  30.453 ms  28.273 ms
 7  142.250.168.220 (142.250.168.220)  28.461 ms  29.476 ms  37.236 ms
 8  * * *
 9  dns.google (8.8.8.8)  74.373 ms  28.131 ms  28.067 ms
```

```
traceroute to 9.9.9.9 (9.9.9.9), 64 hops max, 40 byte packets
 1  172.20.10.1 (172.20.10.1)  11.073 ms  3.798 ms  3.335 ms
 2  * * *
 3  * * *
 4  tamnal-gw1.fi.elisa.net (139.97.12.223)  67.276 ms  27.050 ms  27.105 ms
 5  pch42.unicast.trex.fi (195.140.192.28)  26.758 ms  35.944 ms  35.032 ms
 6  dns9.quad9.net (9.9.9.9)  26.928 ms !Z  28.171 ms !Z  27.126 ms !Z
ashifmoon@Ashifs-MacBook-Air ~ %
```

```
ashifmoon@Ashifs-MacBook-Air ~ % nslookup reliefweb.int
Server:         fe80::50b1:27ff:fe42:8b64%12
Address:        fe80::50b1:27ff:fe42:8b64%12#53

Non-authoritative answer:
Name:   reliefweb.int
Address: 18.233.47.37
Name:   reliefweb.int
Address: 44.208.54.121
Name:   reliefweb.int
Address: 44.194.187.7

ashifmoon@Ashifs-MacBook-Air ~ % traceroute 44.194.187.7
traceroute to 44.194.187.7 (44.194.187.7), 64 hops max, 40 byte packets
 1  172.20.10.1 (172.20.10.1)  9.393 ms  4.232 ms  3.483 ms
 2  * * *
 3  * * *
 4  * * *
 5  213.192.184.80 (213.192.184.80)  70.789 ms  27.066 ms  26.749 ms
 6  213.192.184.95 (213.192.184.95)  32.195 ms  40.373 ms  47.111 ms
 7  sto-b9-link.ip.twelve99.net (213.248.100.236)  47.908 ms *  77.593 ms
 8  sto-bb2-link.ip.twelve99.net (62.115.139.186)  43.843 ms  32.961 ms  43.905 ms
 9  kbn-bb6-link.ip.twelve99.net (62.115.139.173)  39.900 ms  48.212 ms  53.990 ms
10  nyk-bb2-link.ip.twelve99.net (80.91.254.91)  204.404 ms  123.273 ms  158.223 ms
11  nyk-b17-link.ip.twelve99.net (62.115.137.15)  160.722 ms *  4055.730 ms
12  *
```

Question14:Use Ficix statistics web page and answer:

- What is the most quiet IP traffic hour in the Ficix 1 exchange point?
- Which organisations or companies are connected to Ficix 3?

Answer 14: The quietest hour for IP traffic at the Ficix 1 exchange point in Espoo varies, but traffic typically drops to its lowest during late-night and early-morning hours, usually around 3:00-4:00 AM, when internet activity is minimal. This is common for internet exchange points, reflecting reduced user activity during these off-peak times(Ficix)(Ficix).
Ficix 3, located in Oulu, connects a variety of organizations, including ISPs and content providers. Some of the notable companies and organizations connected to Ficix nodes (including Ficix 3) are NORDUnet, which supports research and education networks, and various other carriers and content providers that leverage Ficix for IP peering(Ficix)(Ficix).

Question 15: List all private IPv4 networks (RFC1918)

Answer 15: Private IPv4 networks, as defined by RFC1918, are reserved for use within private networks and are not routable on the public internet. These address ranges are:

1. 10.0.0.0/8: Includes all addresses from 10.0.0.0 to 10.255.255.255.
2. 172.16.0.0/12: Includes all addresses from 172.16.0.0 to 172.31.255.255.
3. 192.168.0.0/16: Includes all addresses from 192.168.0.0 to 192.168.255.255.

These address ranges are commonly used in local area networks (LANs) and are handled by routers that use network address translation (NAT) to manage traffic between the private network and the public internet.

Question 16: What is the purpose of IPv4 private networks?

Answer 16: The purpose of IPv4 private networks is to allow organizations and individuals to use IP addresses within their internal networks without conflicting with publicly routable IP addresses on the internet. These private addresses, as defined by RFC1918, are specifically reserved for internal communication within local area networks (LANs) and are not routable on the public internet.

Here are the key purposes:

Conservation of IPv4 Addresses: Since the global pool of IPv4 addresses is limited, private IP ranges help conserve public addresses by allowing millions of devices to communicate internally without consuming unique public IPs.

Network Security: By using private IP addresses, devices within a network are shielded from direct access by external internet users. Instead, a Network Address Translation (NAT) mechanism allows controlled access between the internal network and the public internet.

Internal Communication: Private networks enable seamless communication within an organization or home network without the need to connect directly to the public internet. This is particularly useful for resource sharing, such as file servers or printers.

Flexibility and Control: Private IP networks offer more flexibility and control for network administrators to set up and manage large internal networks. They can create as many devices or subnets as necessary using the private address ranges.

By using private IP addresses, businesses and individuals can effectively structure large, scalable networks without exhausting the limited pool of public IPv4 addresses.

Question 17:List and explain three or more purposes and features of the ICMP and or ICMPv6 protocol

Answer 17: ICMP and ICMPv6: The Network's Traffic Cops
Think of ICMP and ICMPv6 as the traffic cops of the internet. They help keep things running smoothly by:

- Reporting problems: When a packet gets lost or can't reach its destination, ICMP sends a message saying, "Hey, there's a problem here!"
- Finding the right path: ICMP can help packets find the best way to get from point A to point B.
- Discovering neighbors: ICMPv6 helps devices on a network find each other.

So, whenever you're browsing the web or streaming a video, ICMP and ICMPv6 are working behind the scenes to make sure everything goes smoothly.

Question 18:Try to solve these basic IP subnet calculations without checking the solutions:

- If network address is 192.168.100.0, and subnet mask is 255.255.255.224, what is the broadcast address of the network?

- If network address is 1.2.3.4, and broadcast address is 1.2.3.7, what is the subnet mask of the network?
- If broadcast address is 192.168.129.255 and network mask is 255.255.254.0, what is the network address of the network?

Answer 18:

Network Address: 192.168.100.0
Subnet Mask: 255.255.255.224
Broadcast Address: 192.168.100.31

Network Address: 1.2.3.4
Broadcast Address: 1.2.3.7
Subnet Mask: 255.255.255.252

Broadcast Address: 192.168.129.255
Subnet Mask: 255.255.254.0
Network Address: 192.168.128.0

Question 19: Try to solve these IP subnetting assignments without checking the solutions and document at least some examples/answers to the learning diary. Answers should contain (for each subnet): Network address, broadcast address and subnet mask:

- Subnetting task 1:
  - The address space available is 172.16.64.0/23. Subnet it and create 5 (A, B, C, D and E) IPv4 subnets with following amount of hosts in each network: A = 85, B = 45, C = 95, D = 57, E = 34.
  - Leave some small amount of free addresses to each subnet. Avoid unnecessary waste of IPs.
- Subnetting task 2:
  - Same as task 1, but available address space is now 192.168.0.0/25 and networks/hosts are: A = 28, B = 10, C = 60, D = 4.
  - Leave some small amount of free addresses to each subnet. Avoid unnecessary waste of IPs.
- Subnetting task 3:
  - IPv6 address space available: 2001:708:510::/48. Create four /64 IPv6 networks.

Answer : Simplified Subnetting Solutions
Subnetting Task 1

- Original Network: 172.16.64.0/23
- Subnets:
  - A: 172.16.64.0/26 (62 hosts)
  - B: 172.16.64.64/27 (30 hosts)
  - C: 172.16.64.96/26 (62 hosts)
  - D: 172.16.64.160/27 (30 hosts)
  - E: 172.16.64.192/28 (14 hosts)

Subnetting Task 2

- Original Network: 192.168.0.0/25
- Subnets:
  - A: 192.168.0.0/27 (30 hosts)
  - B: 192.168.0.32/29 (6 hosts)

    - C: 192.168.0.40/26 (62 hosts)
    - D: 192.168.0.64/30 (2 hosts)

Subnetting Task 3

- Original Network: 2001:708:510::/48
- Subnets:
    - A: 2001:708:510::/64
    - B: 2001:708:510:1::/64
    - C: 2001:708:510:2::/64
    - D: 2001:708:510:3::/64

Note: In each task, we've chosen subnet masks that provide the requested number of hosts while minimizing wasted addresses. The numbers in parentheses represent the maximum number of hosts available in each subnet.

…

Week 3

Question 20: Use Linux or Windows command line telnet or any other TCP socket client application (install Putty or any telnet client if needed) to access the TCP service in pouta.ipt.oamk.fi listening TCP port 55555. What is the text string the server replies to your TCP connection if you send some plain text string + newline to it?

Answer 20

```
telnet> telnet pouta.ipt.oamk.fi 55555
Trying 195.148.31.57...
Connected to pouta.ipt.oamk.fi.
Escape character is '^]'.
Hello from Din22sp
Upper case reply: HELLO FROM DIN22SP
Connection closed by foreign host.
ashifmoon@Ashifs-MacBook-Air ~ % telnet
telnet> ^C
ashifmoon@Ashifs-MacBook-Air ~ % telnet pouta.ipt.oamk.fi 55555

Trying 195.148.31.57...
Connected to pouta.ipt.oamk.fi.
Escape character is '^]'.
Hello
Upper case reply: HELLO
Connection closed by foreign host.
ashifmoon@Ashifs-MacBook-Air ~ % nc pouta.ipt.oamk.fi 55555

hello
Upper case reply: HELLO
ashifmoon@Ashifs-MacBook-Air ~ %
```

:

Question 21: Answer these questions:

- Explain shortly the purpose of TCP acknowledgment and sequence numbers
- What is the purpose of TCP SYN bit?
- What is the purpose of TCP reset bit?
- When TCP retransmissions occur?
- What is flow-control? (for IP family protocols such as TCP)
- Explain TCP connection state LISTENING
- Explain TCP connection state ESTABLISHED
- What is the purpose of TCP or UDP source port?
- What is the purpose of TCP or UDP destination port?
- What are the common well-known network service names for these TCP ports: 22, 23, 25, 80, 443, 3306?
- What are common connection-oriented protocol features/advantages, and why TCP is such protocol?
- What are connectionless protocols features (or lack of), and why UDP is connectionless protocol?
- Why most services using UDP prefer max 512 byte UDP datagrams?
- When it is more reasonable to use UDP instead of TCP?
- What is the length of TCP header without extra options? What about UDP header?
- What is TCP Nagle's algorithm? When it should be disabled for networking applications?
- What is Maximum Transmission Unit (MTU) and IPv4 fragmentation?

- What is a raw socket?
- What is port forwading?

Answer 21:

Purpose of TCP Acknowledgment and Sequence Numbers

- TCP Acknowledgment (ACK): Ensures reliability by confirming receipt of data. Each ACK specifies the next byte expected from the sender.
- TCP Sequence Numbers: Track the order of bytes in the data stream, ensuring proper sequencing and allowing reassembly of data at the receiver.

Purpose of TCP SYN Bit

The SYN (Synchronize) bit is used during the three-way handshake to initiate a TCP connection. It is set in the first packet sent by the client to synchronize sequence numbers between the client and server.

Purpose of TCP Reset (RST) Bit
The RST bit signals an immediate termination of the connection, usually when something goes wrong (a host is unreachable or an invalid connection attempt occurs).

When TCP Retransmissions Occur
TCP retransmits data if the sender doesn't receive an acknowledgment (ACK) within a certain timeout (RTT). This ensures reliable data transmission even in cases of packet loss.

What is Flow-Control? (TCP/IP)
Flow control in TCP manages the rate of data transmission between sender and receiver to prevent overwhelming the receiver's buffer. This is achieved using the window size field, allowing the receiver to signal how much data it can handle.

TCP Connection State LISTENING
In the LISTENING state, a server's socket is waiting for incoming connection requests. The server is open to receiving a SYN packet from clients.

TCP Connection State ESTABLISHED
The ESTABLISHED state signifies that a TCP connection is successfully created between client and server, and data can be transmitted between them.

Purpose of TCP/UDP Source Port
The source port identifies the sending application on a client. It allows multiple services or applications on the same device to communicate over the network simultaneously.

Purpose of TCP/UDP Destination Port
The destination port specifies the receiving service or application on the server. Different well-known services listen on specific destination ports.

Common Well-Known Network Service Names for TCP Ports

- 22: SSH (Secure Shell)
- 23: Telnet
- 25: SMTP (Simple Mail Transfer Protocol)
- 80: HTTP (HyperText Transfer Protocol)

- 443: HTTPS (HTTP Secure)
- 3306: MySQL Database

Connection-Oriented Protocol Features/Advantages (Why TCP?)
TCP provides:

- Reliable data transfer through acknowledgments and retransmissions.
- Ordered delivery of packets.
- Error detection and correction. These features make TCP suitable for applications requiring accuracy, such as file transfers.

Connectionless Protocol Features (Why UDP is Connectionless?)
UDP is simpler and faster because:

- It doesn't establish connections before sending data.
- It doesn't provide error correction or ordered delivery, leaving these tasks to the application.
- It's suitable for real-time applications like video streaming or DNS, where speed matters more than reliability.
-

Why Most Services Using UDP Prefer Max 512 Byte UDP Datagrams?

Many services (e.g., DNS) limit UDP datagram sizes to 512 bytes to ensure they fit within a single IP packet and avoid fragmentation, which can introduce latency and loss.

When to Use UDP Instead of TCP?
Use UDP when low latency is more critical than reliability, such as in real-time applications (e.g., VoIP, online gaming, or live streaming) where lost packets don't need to be retransmitted.

Length of TCP and UDP Headers

- TCP Header: 20 bytes without extra options.
- UDP Header: 8 bytes.

What is TCP Nagle's Algorithm?

Nagle's algorithm minimizes the number of small packets sent by combining multiple smaller segments into one large segment. It should be disabled in low-latency applications (gaming or interactive applications) where small, immediate packets are essential.

What is Maximum Transmission Unit (MTU) and IPv4 Fragmentation?

- MTU: The largest packet size that can be transmitted over a network interface without fragmentation.
- IPv4 Fragmentation: If a packet exceeds the MTU, it is broken into smaller fragments for transmission, and reassembled at the destination.
-

What is a Raw Socket?

A raw socket allows applications to bypass the TCP/UDP layers and directly handle lower-level network protocols, useful for custom network protocols or network analysis.

What is Port Forwarding?
Port forwarding redirects traffic from one port on a device (often a router) to another port on a different device. It's commonly used to allow access to services running on internal networks from the internet.
These concepts are fundamental to understanding how the TCP/IP protocol suite functions in network communication.

Question 22: Describe these protocols or services shortly:

- IPSec
- RTP and RTCP
- QUIC (IETF)
- Wireguard
- DoH
- Round-robin DNS
- LDAP
- Radius
- Syslog
- NTP
- SNMP
- SMTP
- SMB/CIFS

Answer 22:

IPSec: A versatile framework for securing IP communications, IPSec provides authentication, integrity, and confidentiality. It can be used to create virtual private networks (VPNs), secure remote access, and protect sensitive data in transit.

RTP: Real-time Transport Protocol (RTP) is the foundation for delivering audio and video data over IP networks. It provides mechanisms for synchronization, quality of service (QoS) control, and payload encapsulation.

RTCP: Real-time Control Protocol (RTCP) complements RTP by providing feedback and control information. RTCP is used to monitor the quality of RTP streams, report packet loss, and control media flow.

QUIC: A new transport layer protocol designed to improve performance and security for web applications, QUIC combines the reliability of TCP with the speed and efficiency of UDP. It introduces features like multiplexing, congestion control, and encryption, making it a promising candidate for future network protocols

WireGuard: A modern VPN protocol known for its simplicity and performance, WireGuard offers a streamlined approach to secure network communication. It's designed to be easy to implement and maintain, making it a popular choice for both personal and enterprise use.

DoH: DNS over HTTPS (DoH) encrypts DNS queries to protect privacy. By encrypting DNS traffic, DoH prevents third parties from monitoring or tracking a user's online activity. This is particularly important in regions with strict internet censorship or where user privacy is a concern.

Round-Robin DNS: A load balancing technique that distributes DNS queries among multiple servers, Round-Robin DNS improves the availability and performance of web applications. By spreading traffic across multiple servers, it reduces the load on individual servers and minimizes downtime.

LDAP: Lightweight Directory Access Protocol (LDAP) is a standard protocol for accessing and managing directory information. LDAP is used to store and retrieve user accounts, group

memberships, and other directory data. It's widely used in enterprise environments for authentication, authorization, and provisioning.
RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a network access control protocol that centralizes authentication, authorization, and accounting (AAA) functions. RADIUS is used to authenticate users, authorize access to network resources, and track usage information.
Syslog: A standard protocol for logging system messages, Syslog provides a centralized way to collect and analyze logs from various devices and applications. This helps IT teams monitor network activity, troubleshoot problems, and detect security threats.
NTP: Network Time Protocol (NTP) synchronizes clocks across a network, ensuring that devices have accurate timekeeping. NTP is essential for many network services, including time-sensitive applications like financial trading and telecommunications.
SNMP: Simple Network Management Protocol (SNMP) is a protocol used for managing network devices. SNMP allows network administrators to monitor device performance, configure settings, and collect statistics.
SMTP: Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending and receiving emails. SMTP defines the rules for exchanging email messages between servers and clients.
SMB/CIFS: Server Message Block (SMB) and Common Internet File System (CIFS) are file sharing protocols used by Windows. SMB/CIFS allow users to access files and folders on remote computers over a network. They are commonly used in business environments for sharing documents, data, and applications.

Question 23: When listing services with netstat command, what is the meaning if some network service is LISTENING and binded to the IP address 127.0.0.1? What if the service is LISTENING IP address 0.0.0.0?

Answer 23: When we use netstat to see what's happening on our network, we might see services listening on these IP addresses:

- 127.0.0.1: This is like our computer's "private address." Only programs on our computer can talk to it. Think of it as a service for our eyes only.
- 0.0.0.0: This is like a public address. Anyone on our network or even the internet can connect to it. This is for services that need to be available to others.

So, if you see a service listening on 127.0.0.1, it's probably something just for you. But if it's listening on 0.0.0.0, be prepared for visitors!

Question 24: Why some applications are using or offer “keepalive” mechanism to maintain established connection (for example SSH connections)?

Answer 24: In network communication, keepalive mechanisms play a crucial role in maintaining established connections, particularly in scenarios where extended periods of inactivity are anticipated. These mechanisms periodically send special packets or messages to ensure that the connection remains active and prevent premature termination due to idle timeouts or network fluctuations.

Keepalives help to avoid connection timeouts that can occur when there's no data exchange for a prolonged period. This is especially important for long-running connections or applications that may experience intermittent inactivity.

By periodically refreshing the connection, keepalives can help to mitigate the impact of network disruptions or temporary connectivity issues. This ensures a more reliable and consistent communication experience.

Keepalives can actually enhance efficiency by reducing the overhead associated with re-establishing connections. By preventing unnecessary connection resets, keepalives can minimize network traffic and improve overall performance.

Keepalives are commonly used in SSH connections to prevent the session from timing out if there's no user activity for a prolonged period. Network devices such as routers and switches often employ keepalive mechanisms to maintain their connections with other devices in the network. Some application-level protocols, such as HTTP and FTP, may also incorporate keepalive mechanisms to improve connection reliability and performance.

Question 25: Study available options with command line command “netstat /?” (Windows) or netstat –help (Linux, maybe MacOS). What different things you can check with netstat command?

Answer 25: Netstat, a versatile command-line utility, is an invaluable asset for network administrators and IT professionals. It provides detailed information about network connections, routing tables, interface statistics, and more. By effectively utilizing netstat, we can:

- Identify active network connections: Determine which processes are communicating with remote systems and the status of those connections (e.g., ESTABLISHED, LISTEN, TIME_WAIT).
- Analyze network traffic: Monitor data transfer rates, packet loss, and other performance metrics to identify potential bottlenecks or congestion issues.
- Troubleshoot network problems: Diagnose connectivity issues, routing problems, and other network-related errors by examining the output of netstat commands.
- Monitor network services: Verify that network services are running and listening on the correct ports.
- Gather network statistics: Collect data on network usage, traffic patterns, and other relevant metrics for analysis and reporting.

Common Netstat Commands and Their Uses:

- netstat -a: Displays all active network connections and listening ports.
- netstat -l: Lists only listening ports.
- netstat -p tcp: Shows TCP connections.
- netstat -s: Provides statistical information about network protocols.
- netstat -r: Displays the routing table.

Question 26: Do the 50 ms mystery quiz from https://mysteries.wizardzines.com/. What was the cause of extra 50 ms delay?

Answer 26: The cause of the extra 50 ms delay in the 50 ms mystery quiz was due to Nagle's algorithm. This algorithm combines small data packets into a single, larger packet to optimize network throughput, but it introduces a small delay while waiting for more data to send.
In this case, the delay was caused by the algorithm waiting to combine smaller packets before sending them out. Disabling Nagle's algorithm resolved the issue and eliminated the extra 50 ms delay

…

Week 4

Question 27: Use Croc to move file or files between two or more hosts/devices. Answer shortly:

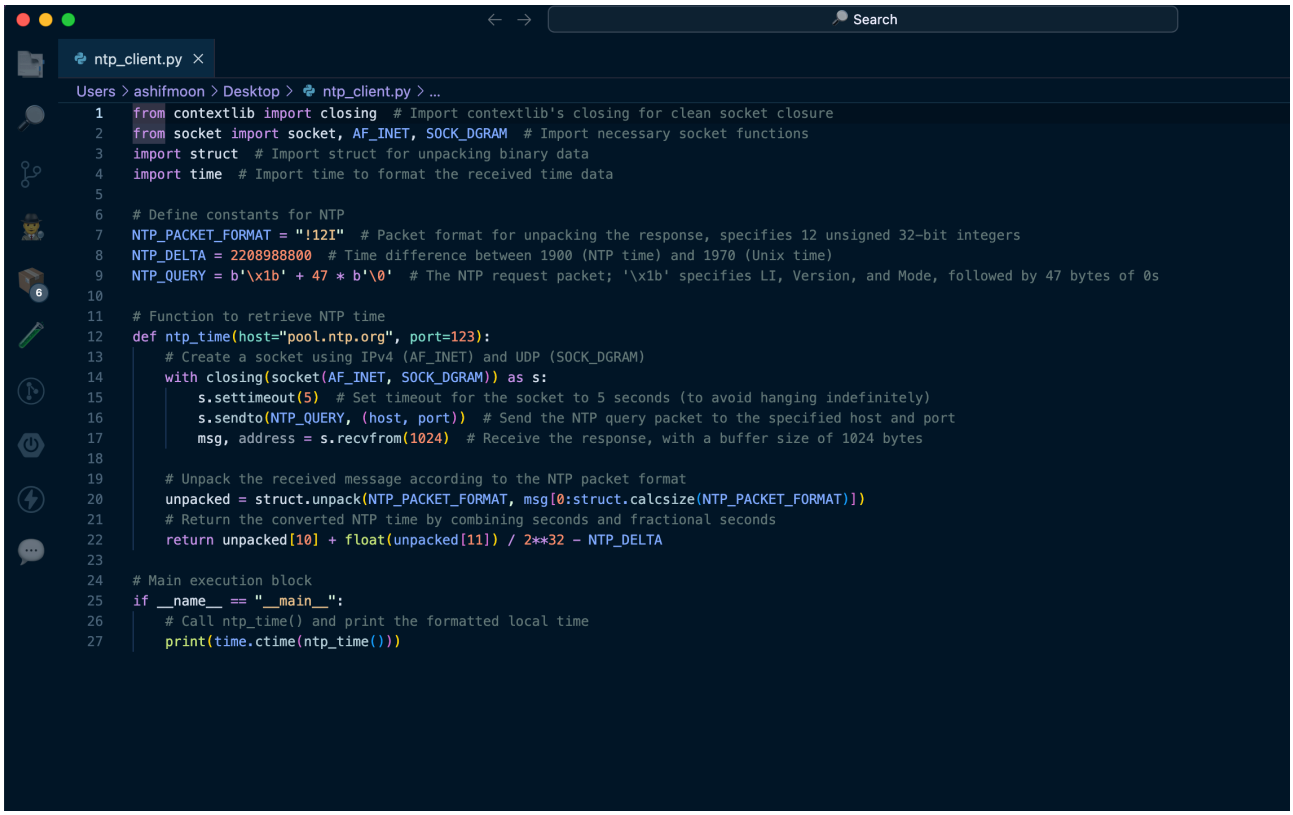
- How the Croc works?
- How the Croc moves files if both hosts are not directly visible to each other? (for example, both are behind NATs or basic firewalls)

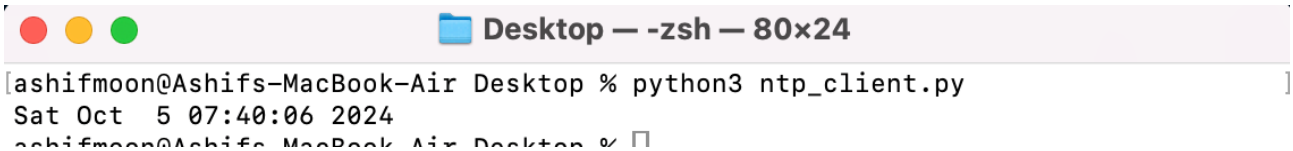
Answer 27: Croc works by establishing a peer-to-peer connection between two devices for file transfer. It uses end-to-end encryption and a relay server to help both hosts communicate, even if they are behind NATs or firewalls.
When both hosts are not directly visible to each other, Croc relies on a relay server to mediate the connection. The relay server helps negotiate the connection between the devices, but the file is still transferred directly between them once the connection is established.

Question 28: Study how NTP protocol operates and analyse this Python NTP client code. Also available here as plain text.

- This Python script uses direct socket programming to access the NTP server. Comment individual socket programming related code lines. Also, answer these:
  - What is the NTP server (DNS) hostname?
  - What is the destination port number being used?
  - Is this Python script using TCP or UDP? How do you know?
  - Try to execute the app with Python

Answer 28:



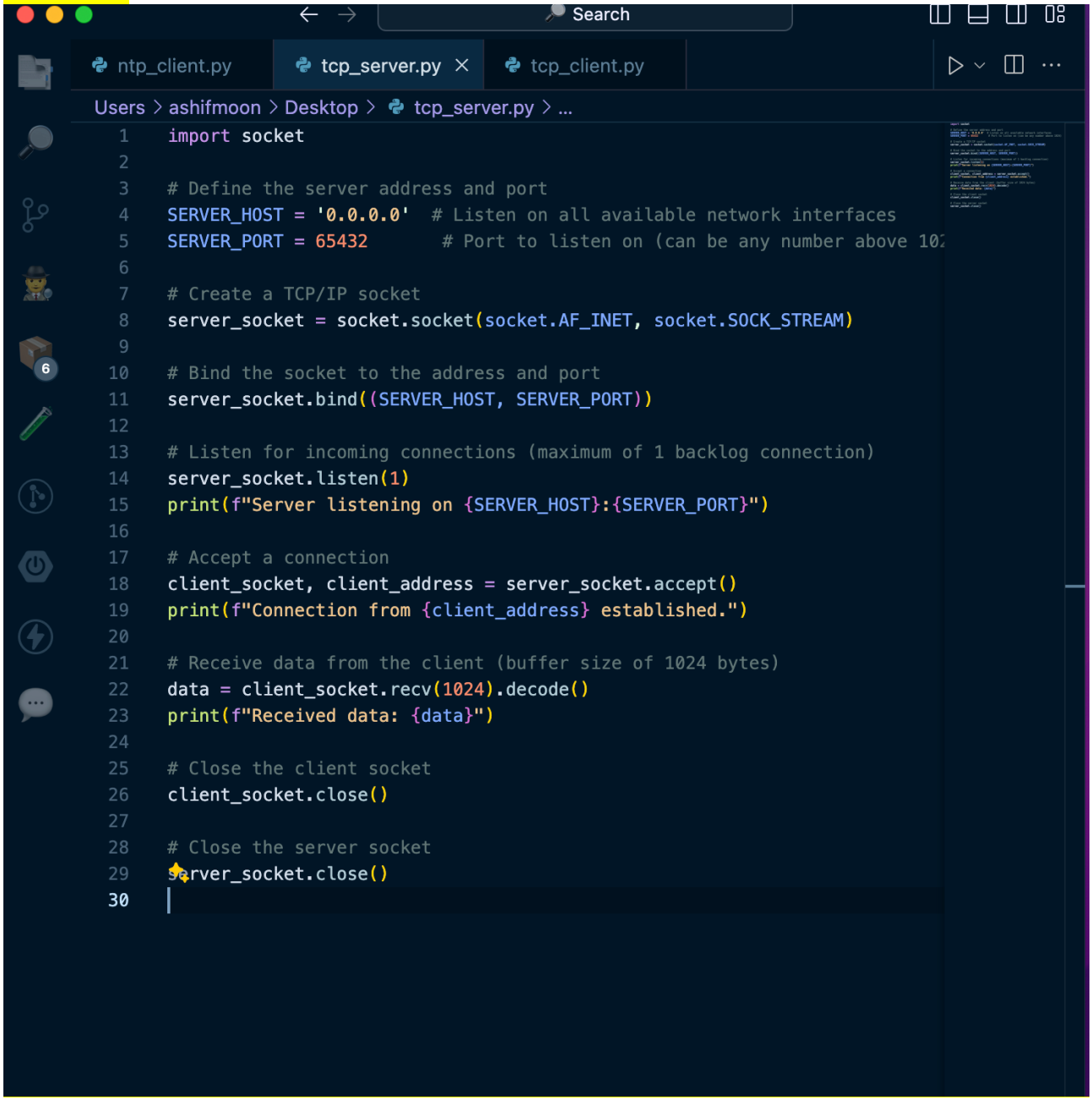


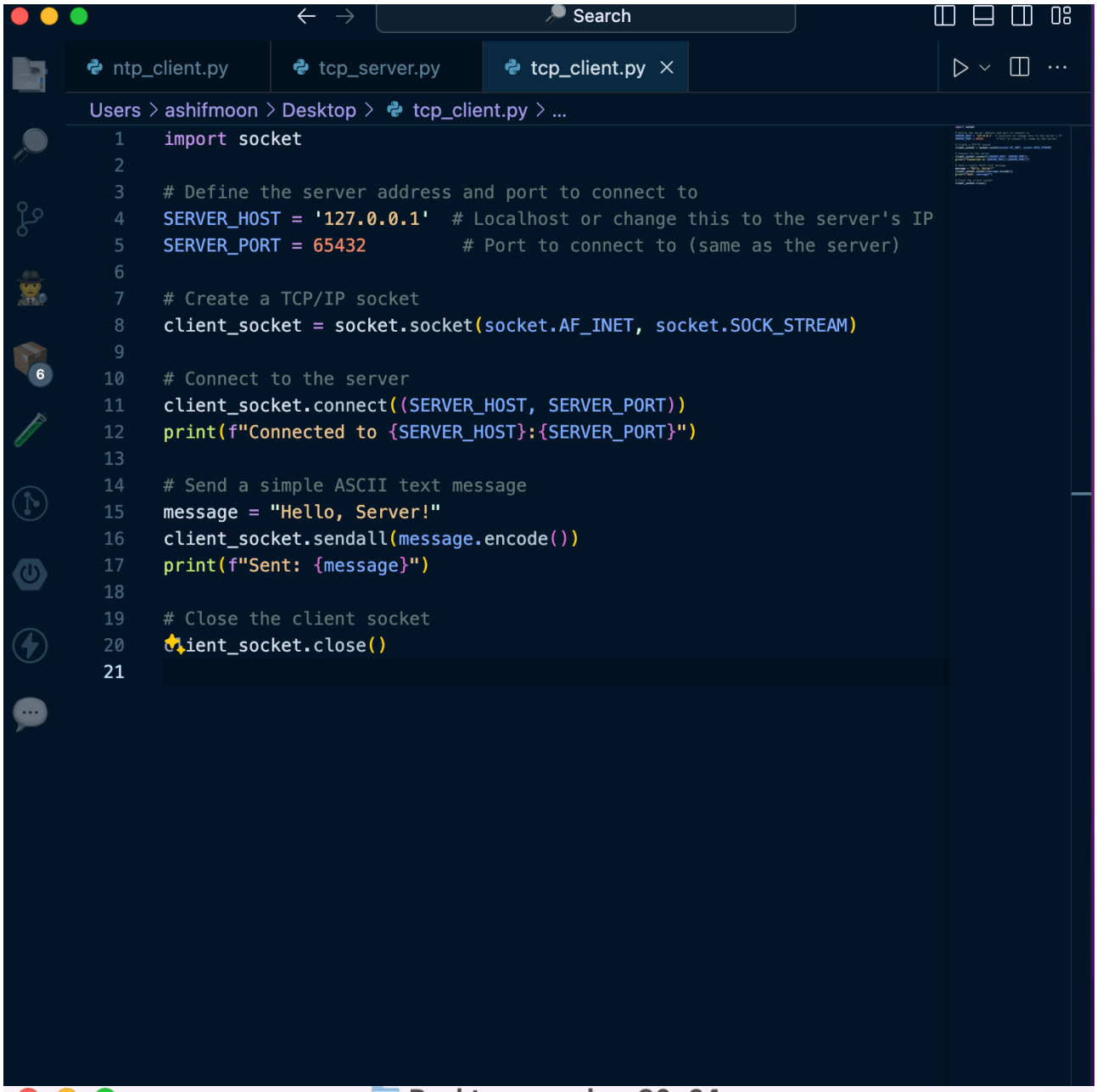
The NTP server's hostname is pool.ntp.org, as specified in the ntp_time function's default argument. The destination port number is 123, which is the default port for NTP. The script is using UDP. This is evident because the socket is created with SOCK_DGRAM, which indicates a UDP socket.

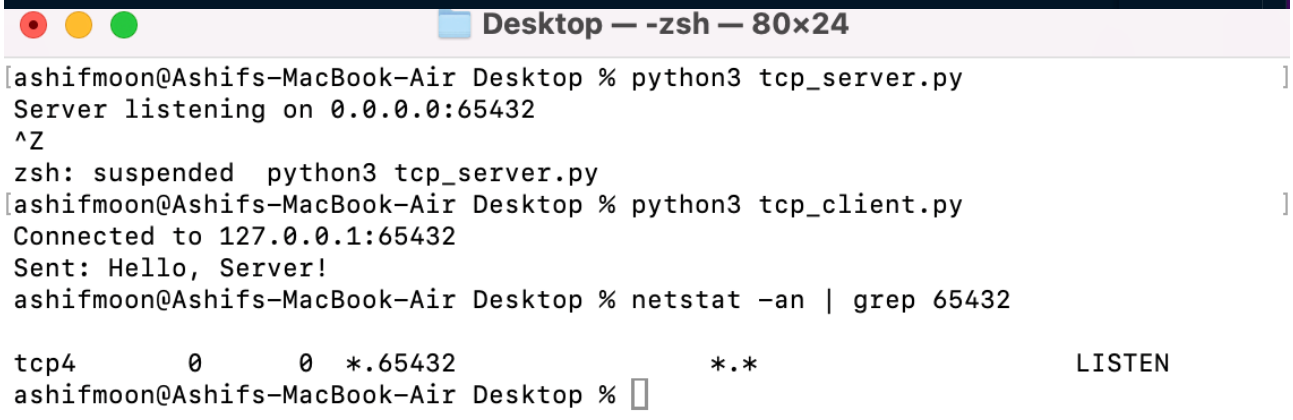
Question 29: Do these Python programming assignments with Windows or Linux (or with MacOS if you want and know how)

- For example, use https://realpython.com/python-sockets/ or similar site(s) for socket programming example codes and create TCP client and TCP server Python scripts
- Establish a TCP connection between your client and server Python scripts (either as localhost traffic or between two separate hosts if you have access to two or more Python running hosts without firewall preventing the traffic)
- Transfer some ASCII text strings between the hosts
  - TCP client connects to the server, sends some plain text string and then disconnects
  - Server prints the text to the console or elsewhere
  - Save your source codes and work. You need scripts again during the course week #5 (Wireshark protocol analyzer assignments)
- Use netstat or similar command line tools to check the TCP connection status (for example the Python server script LISTENING the selected TCP port)

Answer 29:


Search
ntp_client.py
tcp_server.py
tcp_client.py
Users > ashifmoon > Desktop > tcp_server.py > ...
import socket
# Define the server address and port
SERVER_HOST = '0.0.0.0' # Listen on all available network interfaces
SERVER_PORT = 65432 # Port to listen on (can be any number above 10
# Create a TCP/IP socket
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
# Bind the socket to the address and port
server_socket.bind((SERVER_HOST, SERVER_PORT))
# Listen for incoming connections (maximum of 1 backlog connection)
server_socket.listen(1)
print(f"Server listening on {SERVER_HOST}:{SERVER_PORT}")
# Accept a connection
client_socket, client_address = server_socket.accept()
print(f"Connection from {client_address} established.")
# Receive data from the client (buffer size of 1024 bytes)
data = client_socket.recv(1024).decode()
print(f"Received data: {data}")
# Close the client socket
client_socket.close()
# Close the server socket
server_socket.close()


Search
ntp_client.py
tcp_server.py
tcp_client.py
Users > ashifmoon > Desktop > tcp_client.py > ...
1 import socket
2
3 # Define the server address and port to connect to
4 SERVER_HOST = '127.0.0.1' # Localhost or change this to the server's IP
5 SERVER_PORT = 65432 # Port to connect to (same as the server)
6
7 # Create a TCP/IP socket
8 client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9
10 # Connect to the server
11 client_socket.connect((SERVER_HOST, SERVER_PORT))
12 print(f"Connected to {SERVER_HOST}:{SERVER_PORT}")
13
14 # Send a simple ASCII text message
15 message = "Hello, Server!"
16 client_socket.sendall(message.encode())
17 print(f"Sent: {message}")
18
19 # Close the client socket
20 client_socket.close()
21


Desktop — -zsh — 80×24
ashifmoon@Ashifs-MacBook-Air Desktop % python3 tcp_server.py
Server listening on 0.0.0.0:65432
^Z
zsh: suspended python3 tcp_server.py
ashifmoon@Ashifs-MacBook-Air Desktop % python3 tcp_client.py
Connected to 127.0.0.1:65432
Sent: Hello, Server!
ashifmoon@Ashifs-MacBook-Air Desktop % netstat -an | grep 65432
tcp4 0 0 *.65432 *.* LISTEN
ashifmoon@Ashifs-MacBook-Air Desktop %

Week 5

Question 30: Define following terms and concepts shortly:

- What is the difference between encoding and encryption?
- List few common encryption algorithms or systems
- List few common encoding systems
- What are plain text protocols? List some
- Encapsulation (protocol)
- JSON, XML, YAML, CSV

Answer 30:

Difference between encoding and encryption:

Encoding is the process of converting data from one format to another, often for transmission or storage purposes. It's about representation. For instance, converting text to binary for computer storage.

Encryption is the process of transforming data into a secret code, making it unreadable to unauthorized parties. It's about security. Encryption uses algorithms to scramble data, requiring a key to decrypt.

Common Encryption Algorithms and Systems

- Symmetric Key Encryption:
  - AES (Advanced Encryption Standard)
  - DES (Data Encryption Standard)
  - 3DES (Triple DES)
  - Blowfish
- Asymmetric Key Encryption:
  - RSA (Rivest-Shamir-Adleman)
  - ECC (Elliptic Curve Cryptography)
  - Diffie-Hellman Key Exchange
  -

Common Encoding Systems

- ASCII (American Standard Code for Information Interchange): Represents characters as 7-bit binary codes.
- UTF-8 (Unicode Transformation Format): A variable-length encoding scheme for Unicode characters.
- Base64: Encodes binary data as a sequence of printable ASCII characters.
- URL Encoding: Encodes special characters in URLs for safe transmission.

Plain Text Protocols

Plain text protocols transmit data in a human-readable format without encryption.

- HTTP (Hypertext Transfer Protocol): Used for web communication.
- FTP (File Transfer Protocol): Used for transferring files between computers.
- SMTP (Simple Mail Transfer Protocol): Used for sending and receiving emails.
- Telnet: A remote login protocol.

Encapsulation (Protocol)

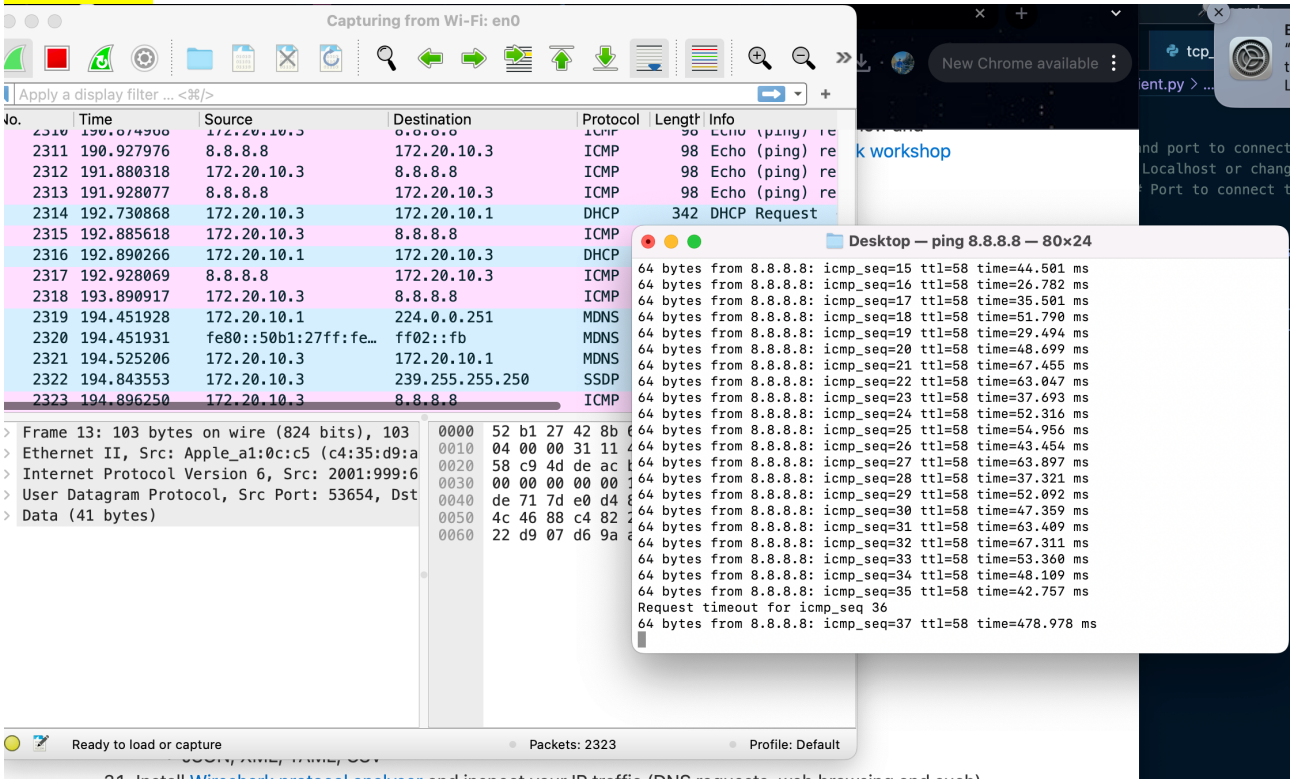
Encapsulation is the process of wrapping data in a packet for transmission. This packet includes headers containing information like the source and destination addresses, protocol type, and error checking data.
JSON, XML, YAML, CSV

- JSON (JavaScript Object Notation): A lightweight data-interchange format.
- XML (Extensible Markup Language): A markup language for structured data.
- YAML (Yet Another Markup Language): A human-readable data serialization language.
- CSV (Comma-Separated Values): A simple format for tabular data.

Question 31: Install Wireshark protocol analyser and inspect your IP traffic (DNS requests, web browsing and such) with the Wireshark:

- Analyse the plain text traffic between the TCP socket Python scripts you did during the course week #4. Note: use localhost network interface when capturing host internal traffic (localhost/127.0.0.1)
- Try to ping 8.8.8.8 from command prompt and capture the traffic. What protocols ping was using? What is the total header length of your ping request (all used protocol headers combined when ping sends echo request)?
- Capture some web browsing traffic and related DNS requests. What are those A (and maybe AAAA requests)? Which protocol is used for DNS requests? (Note: This cannot be done with web browser if your browser uses DNS over HTTPS. Most do now. Either skip this task or disable DoH temporary in the web browser settings)

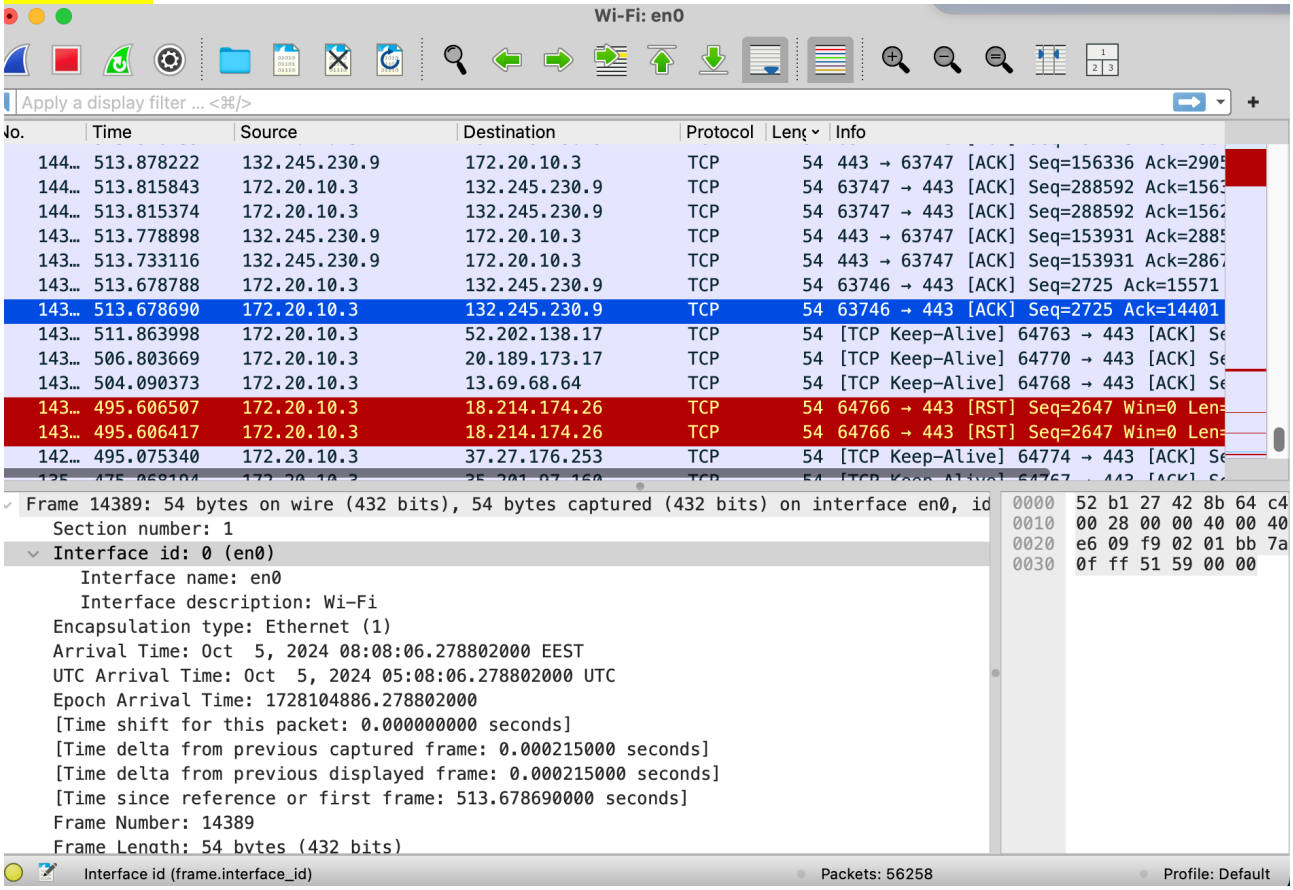
Answer 31:



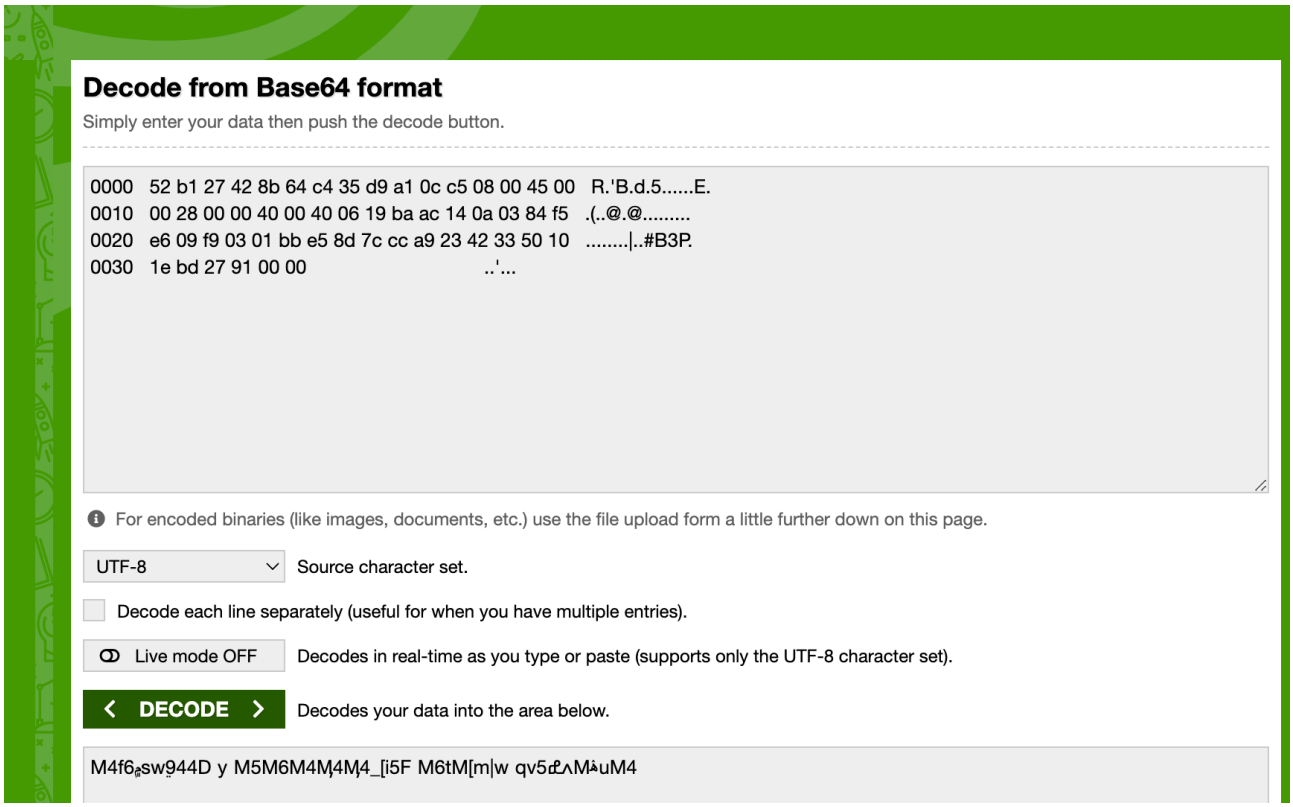
Question 32: Download this zipper pcap traffic file and inspect it with Wireshark. The IP traffic sample is about IoT device sending base64 encoded and JSON formatted data to a server. Answer these questions:

- What is the total size of captured frame in bits?
- What is the payload length (data) in bytes?
- What is the source IP address of device sending the traffic?
- What is the destination IP address receiving the traffic?
- What is the IP family procotol delivering the data?
- What is the source port?
- What is the destination port?
- Extract the payload as printable text (use right mouse button and copy as printable text for the data part only). Use any base64 decoder to convert the data to a plain text JSON message. What is the content of JSON formatted data?

Answer 32:



Frame 432 bits
Payload length 20 bytes
Source address 172.20.10.3
Destination address 132.245.230.9
IP family protocol: V4
Source port 63747
Destination port 443



Question 33: Download this zipper pcap traffic file and inspect it with Wireshark. Traffic is simple MySQL session example from Wireshark Wiki. Answer these questions:

- What is the destination IP address receiving the traffic?
- What is the destination TCP port?
- Use Wireshark's follow TCP stream feature (right mouse button) and inspect what are the two database rows (animals) and related values which were inserted to the foo table's animal and name columns?

Answer 33:
Destination Address:192.168.0.254
TCP port 3306

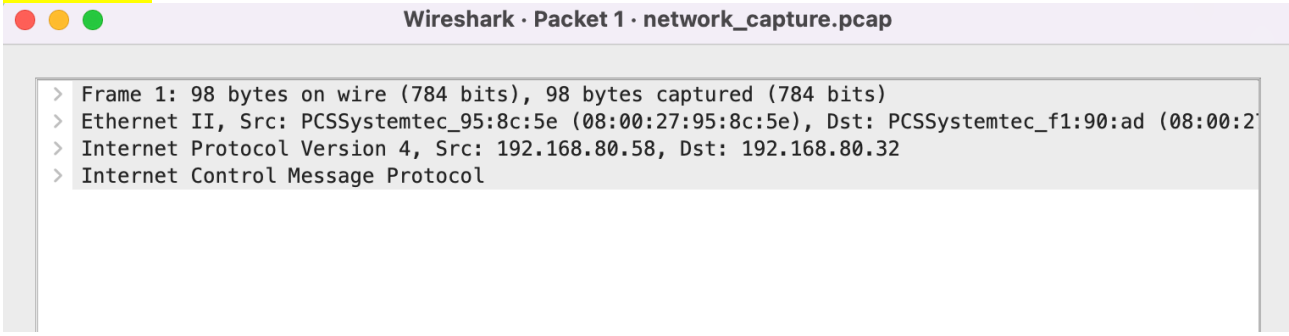

Wireshark · Follow TCP Stream (tcp.stream eq 0) · mysql_complete.pcap
.....'....def....@@version_comment..!.K.....................Gentoo Linux mysql-5.0
.54.........
.....SELECT DATABASE()
....def...
DATABASE()..!.f.............................
.....test
....
.....show databases
.....1....def..SCHEMATA..Database.SCHEMA_NAME.!.................".....information_
schema.....test.......".
.....show tables
.....9....def..TABLE_NAMES..Tables_in_test
TABLE_NAME.!.................".....agent.......".
.....agent.
*....def.test.agent.agent.id.id.?.......B....0=....def.test.agent.agent.custom_data1
.custom_data1.!.h..........=....def.test.agent.agent.custom_data2.custom_data2.!.h..
........=....def.test.agent.agent.custom_data3.custom_data3.!.h...................
.....create table foo (id BIGINT(10) UNSIGNED NOT NULL AUTO_INCREMENT PRIMARY KEY,
animal VARCHAR(64) NOT NULL, name VARCHAR(64) NULL DEFAULT NULL) ENGINE = MYISAM
....
7....insert into foo (animal, name) values ("dog", "Goofy")
....
:....insert into foo (animal, name) values ("cat", "Garfield")
....
.....select * from foo
.....$....def.test.foo.foo.id.id.?.
....#B...,....def.test.foo.foo.animal.animal.!...........(....def.test.foo.foo.name.
name.!.................".....1.dog.Goofy.....2.cat.Garfield.......".
'....delete from foo where name like '%oo%'
.......".
.....delete from foo where id = 1
....
.....select count(*) from foo
..........def....count(*)..?.........................1.........
.....select * from foo
.....$....def.test.foo.foo.id.id.?.
....#B...,....def.test.foo.foo.animal.animal.!...........(....def.test.foo.foo.name.
name.!.........................2.cat.Garfield.........
.....delete from foo
....
.....drop table foo
....
.....
18 client pkts, 18 server pkts, 35 turns.
Entire conversation (1853 byte
Show as
ASCII
No delta times
Stream
0
Find:
Case sensitive
Find Next

...

Question 34:Download this zipped pcap traffic file and inspect it with Wireshark. Traffic has been captured from host 192.168.80.32. Answer these questions:

- What is the MAC address of host 192.168.80.32?
- What is the MAC address of host 192.168.80.1? Which vendor has build the ethernet chipset of host 192.168.80.1? (use Wireshark or IEEE OUI data)
- Which IP address sent ICMP echo requests to this (192.168.80.32) host? Also, there is a repeating short message inside ICMP datagrams the host sent as ICMP echo request payload. What is the repeated message?
- What was the web page the host 192.168.80.32 visited first (full web page address, not just the host)? What was the web browser or HTTP user agent string used to access that web server?
- What is the hostname in "Host:" field of the HTTP GET request sent by 192.168.80.32?
- What is most likely the default DNS server (the IP address) used by the host 192.168.80.32?
- Use Wireshark's file/export objects/HTTP feature to extract the ZIP file which was downloaded from the web server 193.167.100.88. What is inside the ZIP file?
- Host 192.168.80.32 sent DNS requests to host 9.9.9.9. What are the requests?

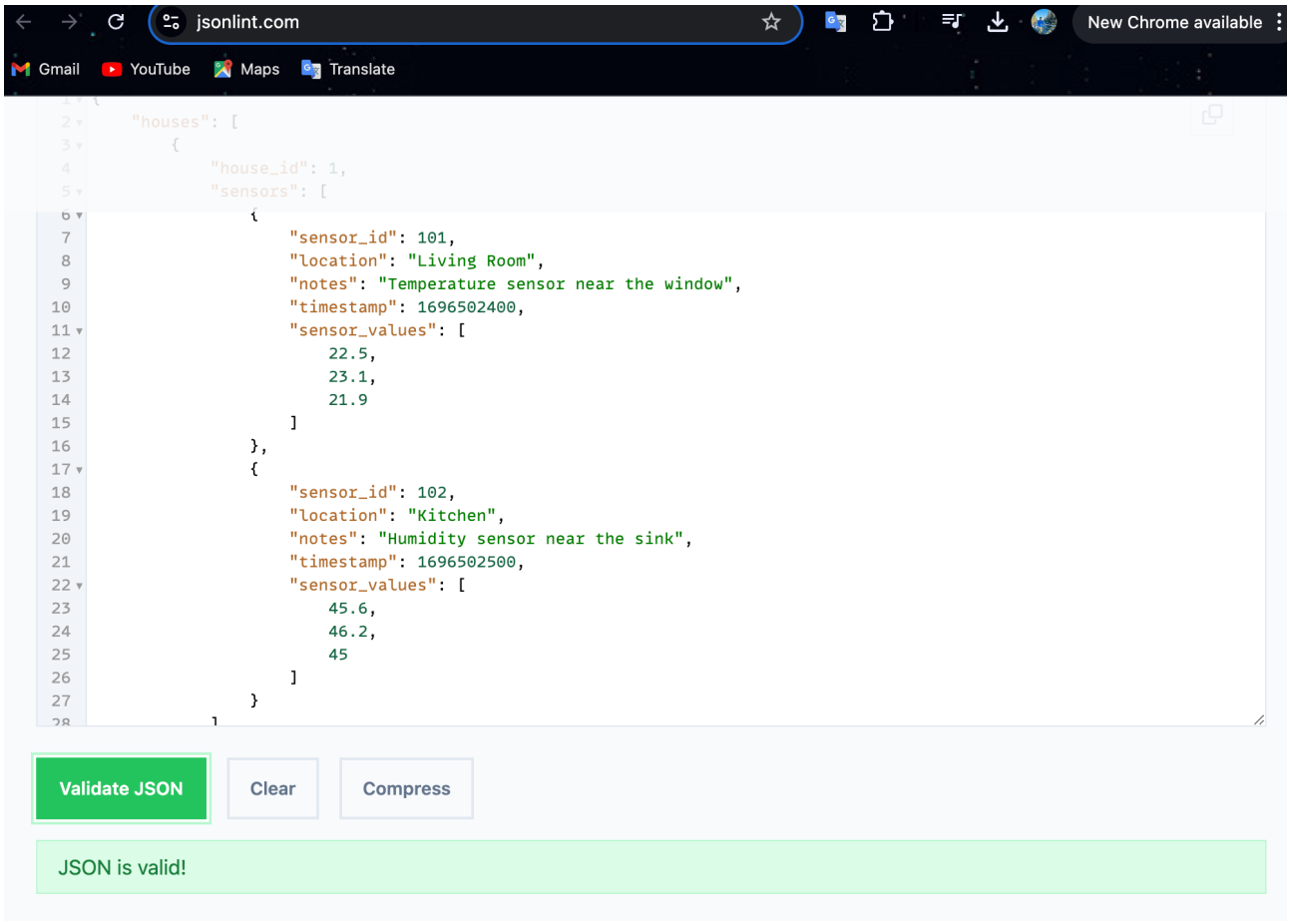
Answer 34:



Question 35:Create a new JSON file with any text editor. JSON file should contain data for at least two houses and related IoT sensor data. Each house must have few sensors with following information and some random data for each sensor. Something like this:

- Validate your JSON file with validator: jsonlint.com or jsonformatter.curiousconcept.com
- What is GraphQL?

Answer 35:



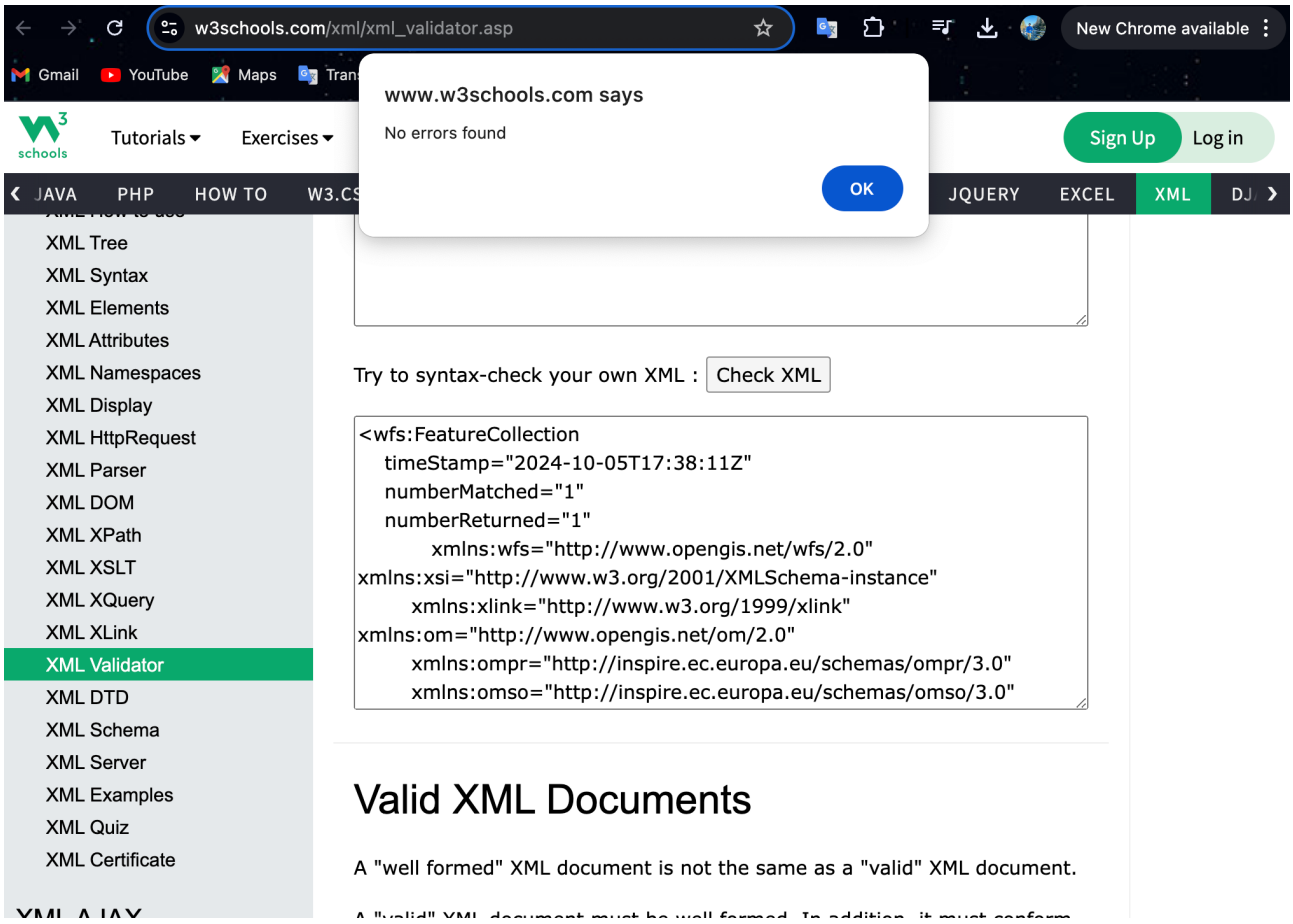
GraphQL is a query language for APIs that provides a flexible and efficient way for clients to request data from a server. Unlike traditional REST APIs, which often require multiple requests to retrieve different data points, GraphQL allows clients to specify exactly what data they need in a single request. GraphQL is widely used in modern web development for its ability to provide a more efficient and flexible way to interact with APIs. It has become a popular choice for building scalable and maintainable applications.

Question 36: Install Cmder (or some other toolset where you have Curl or similar tool to make HTTP requests from command line or application.) Use Curl to fetch XML formatted weather data from FMI:

- Inspect and validate the received XML data with www.w3schools.com/xml/xml_validator.asp

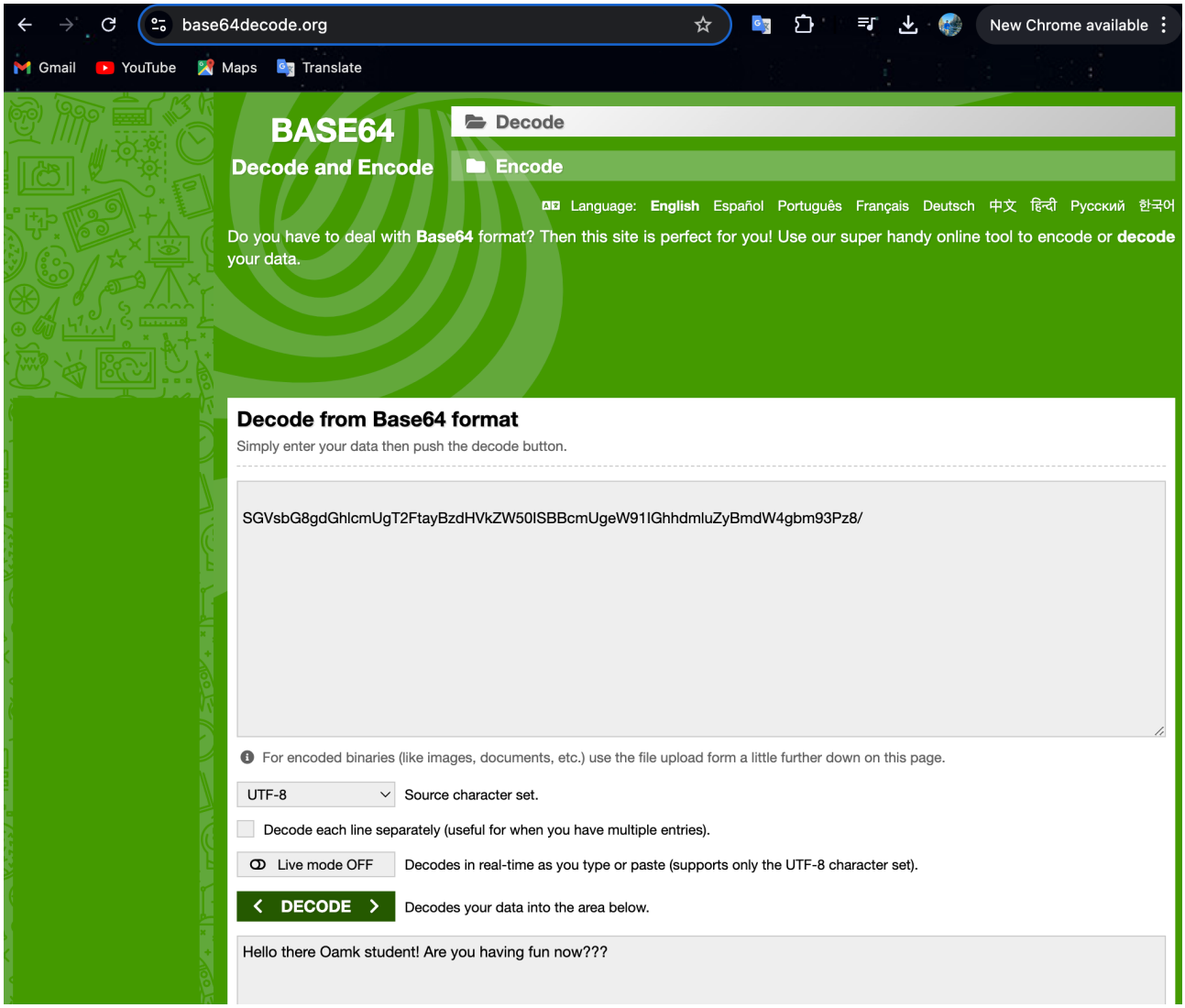
Answer 36:

```
ashitmoon@Ashits-MacBook-Air Desktop % curl -s -L "https://opendata.fmi.fi/wfs?r
equest=getFeature&storedquery_id=fmi::observations::weather::timevaluepair&place
=oulu&timestep=100&parameters=temperature"
<?xml version="1.0" encoding="UTF-8"?>
<wfs:FeatureCollection
    timeStamp="2024-10-05T17:38:11Z"
    numberMatched="1"
    numberReturned="1"
          xmlns:wfs="http://www.opengis.net/wfs/2.0" xmlns:xsi="http://www.w3.o
rg/2001/XMLSchema-instance"
        xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:om="http://www.opengis.
net/om/2.0"
        xmlns:ompr="http://inspire.ec.europa.eu/schemas/ompr/3.0"
        xmlns:omso="http://inspire.ec.europa.eu/schemas/omso/3.0"
        xmlns:gml="http://www.opengis.net/gml/3.2" xmlns:gmd="http://www.isotc21
1.org/2005/gmd"
        xmlns:gco="http://www.isotc211.org/2005/gco" xmlns:swe="http://www.openg
is.net/swe/2.0"
        xmlns:gmlcov="http://www.opengis.net/gmlcov/1.0"
        xmlns:sam="http://www.opengis.net/sampling/2.0"
        xmlns:sams="http://www.opengis.net/samplingSpatial/2.0"
        xmlns:wml2="http://www.opengis.net/waterml/2.0"
        xmlns:target="http://xml.fmi.fi/namespace/om/atmosphericfeatures/1.1"
        xsi:schemaLocation="http://www.opengis.net/wfs/2.0 http://schemas.opengi
```



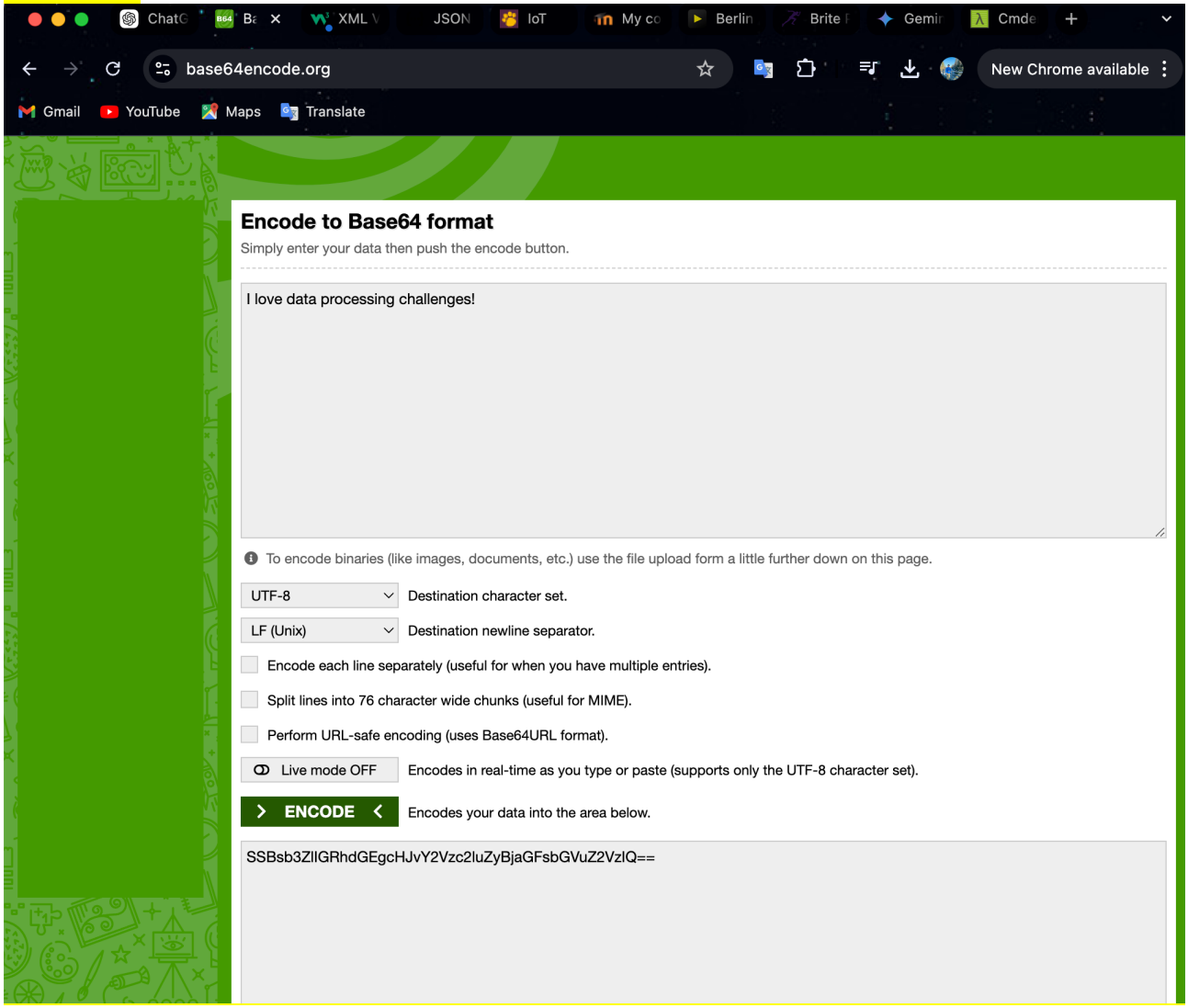
Question 37 Decode this base64 encoded message with any tool(s) you prefer:
SGVsbG8gdGhlcmUgT2FtayBzdHVkZW50ISBBcmUgeW91IGhhdmluZyBmdW4gbm93Pz8/

Answer 37:



Question 38: Encode this string:“I love data processing challenges!” with base64 encoding

Answer 38:


base64encode.org
New Chrome available
Gmail
YouTube
Maps
Translate
Encode to Base64 format
Simply enter your data then push the encode button.
I love data processing challenges!
To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8
Destination character set.
LF (Unix)
Destination newline separator.
Encode each line separately (useful for when you have multiple entries).
Split lines into 76 character wide chunks (useful for MIME).
Perform URL-safe encoding (uses Base64URL format).
Live mode OFF
Encodes in real-time as you type or paste (supports only the UTF-8 character set).
ENCODE
Encodes your data into the area below.
SSBsb3ZlIGRhdGEgcHJvY2Vzc2luZyBjaGFsbGVuZ2VzIQ==

Week 6

Question 39: Describe the difference between request-response and publish-subscribe communication models

Answer 39:
Request-Response and Publish-Subscribe are two fundamental communication paradigms employed in distributed systems. They differ significantly in their approach to message exchange and the nature of the sender-receiver relationship.
Request-Response

- Sender-Receiver Relationship: A direct, one-to-one relationship exists between the sender (client) and receiver (server).
- Message Exchange: The sender initiates communication by sending a request message to the receiver. The receiver processes the request and sends a response message back to the sender.
- Use Cases: Commonly employed in scenarios where a client requires a specific response to a query, such as database queries, web requests, or Remote Procedure Calls (RPCs).

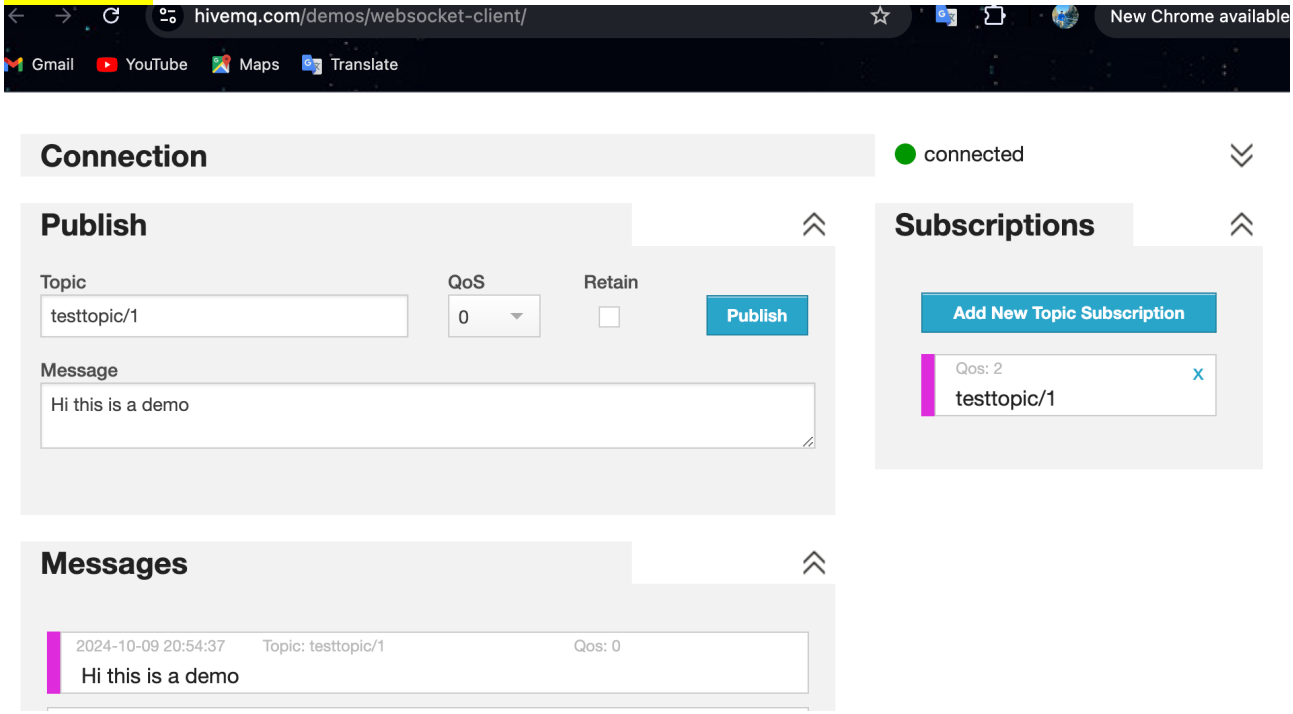
Publish-Subscribe

- Sender-Receiver Relationship: A one-to-many or many-to-many relationship. The sender (publisher) broadcasts a message to multiple receivers (subscribers).
- Message Exchange: The publisher sends a message to a topic or channel. Subscribers interested in that topic subscribe to it and receive the message.
- Use Cases: Well-suited for scenarios where a single event or data update needs to be disseminated to multiple interested parties, such as real-time updates, messaging systems, and event-driven architectures.

Question 40: Try MQTT websocket demo application

- Subscribe to some existing topic(s) in HiveMQ demo service
- Publish some messages to the topic(s) you subscribed

Answer 40:



Question 41: Explain what are MQTT retained messages

Answer 41: In MQTT, retained messages are a special type of message that remain stored on the MQTT broker, even after they are delivered to the subscribers. These messages are useful when you want to ensure that new subscribers to a topic immediately receive the most recent message published to that topic, without waiting for a new one to be published.

When a client publishes a message to a topic with the retained flag set to true, the MQTT broker stores that message as the "last known good value" for that topic.When a new client subscribes to that topic, the broker immediately sends the retained message to the subscriber, so the subscriber gets the most up-to-date data right away.Subsequent messages published to that topic without the retained flag do not overwrite the retained message. However, if a new retained message is published to the same topic, it replaces the old one.If a publisher sends a retained message with an empty payload, the broker will delete the retained message for that topic.

Retained messages are particularly useful in scenarios where the last known state of a device or sensor needs to be communicated to new subscribers right away.

Question 42: List shortly some reasons why MQTT may be better than HTTP for IP-based IoT communication? (For example: HTTP vs. MQTT: A tale of two IoT protocols and MQTT Vs. HTTP: Understanding the Differences)

Answer 42: Here are some key reasons why MQTT may be better than HTTP for IP-based IoT communication:

1. Lightweight Protocol: MQTT uses less bandwidth and has a smaller packet size, making it ideal for devices with limited network resources, unlike HTTP which is more verbose.

2. Efficient Power Consumption: MQTT's low overhead and ability to maintain long-lived connections (with keep-alive messages) make it more power-efficient, important for battery-operated IoT devices.
3. Asynchronous Communication: MQTT is event-driven and uses the publish-subscribe model, which allows devices to communicate without polling, unlike HTTP's request-response model that requires constant polling for updates.
4. Reliable Messaging: MQTT supports Quality of Service (QoS) levels, ensuring messages are delivered reliably depending on the use case. HTTP lacks built-in message delivery guarantees.
5. Persistent Sessions: MQTT allows for session persistence and the use of retained messages, so clients can receive the latest messages immediately after reconnecting, which HTTP doesn't support.
6. Scalability: Due to its low overhead and efficient message delivery mechanism, MQTT can scale better with a large number of devices, compared to the resource-intensive nature of HTTP.

These characteristics make MQTT highly suitable for IoT environments, especially those requiring reliable, low-latency, and efficient communication over constrained networks.

Question 43: What is CoAP?
Answer 43: CoAP (Constrained Application Protocol) is a lightweight protocol designed specifically for use in IoT (Internet of Things) environments, where devices are resource-constrained (e.g., limited power, processing capability, and memory) and networks have low bandwidth. CoAP is intended for machine-to-machine (M2M) communication, particularly in constrained devices and networks, and operates over UDP (User Datagram Protocol). CoAP is standardized by the IETF (Internet Engineering Task Force) as RFC 7252, and it's becoming a popular choice for IoT systems where lightweight, efficient, and low-power communication is critical.

Quesstion 44:What is 6LoWPAn?
Answer 44: 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is a protocol suite that enables IPv6 communication over low-power, low-bandwidth wireless networks, such as those used in Internet of Things (IoT) devices. It is designed to address the challenges of connecting constrained devices to the internet.6LoWPAN initially came into existence to overcome the conventional methodologies that were adapted to transmit information. But still, it is not so efficient as it only allows for the smaller devices with minimal processing ability to establish communication using one of the Internet Protocols, i.e., IPv6. It has very low cost, short-range, low memory usage, and low bit rate. 6LoWPAN provides a robust and efficient solution for connecting constrained devices to the internet, opening up new possibilities for IoT applications across various domains. By addressing the limitations of low-power, low-bandwidth wireless networks, 6LoWPAN enables seamless communication and data exchange between devices and the broader internet ecosystem.

Question 45: What is IETF ROLL?

Answer 45: IETF ROLL (Routing Over Low power and Lossy networks) is a working group within the Internet Engineering Task Force (IETF) that focuses on developing routing protocols tailored for low-power and lossy networks (LLNs). LLNs are networks composed of devices that have limited resources (such as battery-powered sensors or actuators) and operate in environments where

the network may be prone to high packet loss, unstable links, and low bandwidth. These networks are common in IoT applications, such as smart homes, industrial monitoring, and environmental sensing.

Key areas of focus for IETF ROLL include:

- Routing protocol development and improvement: Contributing to the advancement of routing protocols such as BGP, OSPF, and IS-IS to enhance network performance and reliability.
- Routing policy standardization: Developing guidelines and best practices for routing policy configuration and management to ensure consistent and secure network operations.
- Layer 2 technology exploration and standardization: Investigating and standardizing layer 2 technologies like Ethernet, VLANs, and bridging to facilitate efficient data transmission and network segmentation.
- Interoperability enhancement: Promoting compatibility and interoperability between different routing and layer 2 technologies to ensure seamless network operations across diverse environments.
- Network operations challenges: Addressing operational challenges related to network management, troubleshooting, and security to maintain the reliability and integrity of the internet infrastructure.

IETF ROLL plays a pivotal role in shaping the future of the internet by driving innovation and standardization in the areas of routing and layer 2 transport. Its work contributes to the overall resilience, scalability, and security of the internet infrastructure, ensuring a reliable and efficient global network.

Question 46: Describe IETF RPL protocol?
Answer 46: IETF RPL (Routing Protocol for Low-Power and Lossy Networks) is a network protocol designed specifically for Internet of Things (IoT) environments characterized by constrained devices with limited power, bandwidth, and processing capabilities. RPL addresses the unique challenges posed by these networks by providing a scalable, energy-efficient, and reliable routing mechanism. IETF RPL provides a robust and efficient routing solution for low-power and lossy networks, addressing the unique challenges posed by IoT environments. By optimizing energy consumption, ensuring reliable data delivery, and scaling to large networks, RPL enables seamless communication and data exchange between constrained devices and the broader internet ecosystem.

Question 47: Why classic computer network protocols like TCP/IP, data formats such as JSON and XML, and security systems like (PKI/HTTPS) won't usually work at all or are not very optimal to be used in resource limited wireless sensor networks (low power and lossy networks)?

Answer 47:
While classic network protocols like TCP/IP, data formats like JSON and XML, and security systems like PKI/HTTPS have been invaluable in traditional internet communication, they often encounter significant challenges when applied to resource-constrained wireless sensor networks (WSNs).
TCP/IP Limitations:

- Overhead: TCP/IP's overhead, including packet headers, acknowledgments, and retransmissions, can be burdensome for devices with limited processing power and bandwidth.

- Statefulness: TCP/IP's stateful nature can consume valuable resources and increase complexity for constrained devices.
- Congestion Control: TCP's congestion control mechanisms, designed for traditional networks, may not be optimal for WSNs with unpredictable network conditions.

Data Format Limitations:

- Verbosity: JSON and XML, while human-readable, can be verbose, leading to increased data transmission overhead.
- Parsing Overhead: Parsing these formats requires significant computational resources, which can be a bottleneck for constrained devices.

Security Limitations:

- Computational Overhead: PKI/HTTPS' cryptographic operations can be computationally intensive for constrained devices.
- Certificate Management: Managing certificates and keys can be complex and resource-consuming in large-scale WSN deployments.

Why These Limitations Matter in WSNs:

- Power Consumption: Excessive overhead and computational demands can significantly shorten the battery life of constrained devices.
- Bandwidth Constraints: The verbosity of traditional protocols and data formats can limit the amount of data that can be transmitted in WSNs.
- Reliability: The reliability mechanisms built into TCP/IP can be overkill and can even exacerbate packet loss and interference in WSNs.

In conclusion, while classic network protocols, data formats, and security systems have served us well in traditional internet communication, they are often ill-suited for the unique challenges of WSNs. More specialized protocols and techniques, such as those developed specifically for IoT applications, are necessary to address the limitations of constrained devices and ensure efficient and reliable communication in WSN environments.

Question 48: What is the MTU challenge for IPv4 and IPv6 over common wireless low power and lossy wireless connections (Hint: Research Zigbee/IEEE 802.15.4 and Bluetooth MTU vs IPv4 or IPv6)?

Answer 48: MTU (Maximum Transmission Unit) challenge for IPv4 and IPv6 over common low-power and lossy wireless connections like Zigbee/IEEE 802.15.4 and Bluetooth arises from the significant difference in the size of packets these wireless technologies can handle versus the larger packet sizes typically used in IP networking.

Challenges:

Fragmentation and Reassembly:

- IPv4/IPv6 Fragmentation: IP packets larger than the MTU of the underlying link layer must be fragmented. In LLNs (low-power and lossy networks), this leads to:
  - Increased Overhead: Fragmentation adds overhead to the packets, as additional headers must be added for each fragment.
  - Higher Packet Loss: In lossy networks, if one fragment is lost, the entire packet must be retransmitted, which increases the chance of communication failures.
  - Energy Costs: Fragmenting and reassembling packets consumes more energy, which is a critical issue in battery-powered devices.
- IPv6 over IEEE 802.15.4: To address this challenge, 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) was introduced. It provides:
  - Header Compression: 6LoWPAN compresses the large IPv6 headers (40 bytes) to fit within the small MTU of IEEE 802.15.4.

- Fragmentation: 6LoWPAN provides its own fragmentation mechanism, allowing large IPv6 packets to be split into smaller fragments that fit within the 802.15.4 frame size.

Energy and Latency Impacts:

- Energy Consumption: Each fragment must be transmitted separately, consuming more energy for both transmission and reassembly at the destination. This is especially problematic in battery-powered IoT devices, where conserving energy is critical.
- Increased Latency: Fragmentation and reassembly increase the overall time it takes to transmit and receive packets. In lossy networks, retransmissions due to packet loss can further increase latency, affecting real-time communication.

Reliability in Lossy Networks:

- In low-power wireless networks, the likelihood of packet loss is higher due to interference, weak signals, and contention for the wireless medium. When packets are fragmented, losing even a single fragment requires the retransmission of the entire packet, making communication less reliable.

Security Implications:

- Fragmented packets are more vulnerable to certain types of attacks, such as fragmentation-based attacks. Reassembly of fragmented packets adds complexity and potential security risks, as attackers can attempt to manipulate fragments.

the MTU challenge in low-power and lossy networks is a critical consideration for running IP-based protocols, and specialized adaptations like 6LoWPAN are necessary to enable IPv6 communication in these constrained environments.

Question 49: Compare and list few HTTP/1.1, HTTP/2 and HTTP/3 differencies and features

Answer 49: HTTP (Hypertext Transfer Protocol) has evolved significantly from HTTP/1.1 to HTTP/2 and now to HTTP/3. Each version introduces new features and improvements to enhance performance, efficiency, and security. Here's a comparison of the key differences and features among these three versions:

1. HTTP/1.1

- Connection Model:
  - Uses a text-based protocol with a request/response model.
  - Each request-response cycle can only use one TCP connection at a time.
  - Persistent connections are introduced (keep-alive) but can still lead to multiple round trips.
- Head-of-Line Blocking:
  - Suffering from head-of-line blocking, where a single slow response can block all subsequent requests over the same connection.
- Chunked Transfer Encoding:
  - Supports chunked transfer encoding for dynamically generated content, allowing data to be sent in segments.
- Caching:
  - Improved caching mechanisms with Cache-Control and Expires headers, but limited compared to later versions.
- Compression:
  - Introduces gzip compression for responses, but lacks header compression.

2. HTTP/2

- Connection Model:

    - Uses binary framing instead of plain text, allowing multiple streams over a single TCP connection. This enables multiplexing of requests/responses.
- Multiplexing:
    - Eliminates head-of-line blocking by allowing multiple requests and responses to be in flight simultaneously over a single connection.
- Header Compression:
    - Introduces HPACK, a header compression format that reduces the overhead of HTTP headers, leading to smaller packet sizes and faster transmissions.
- Server Push:
    - Supports server push, allowing servers to send resources (e.g., images, CSS files) to the client proactively without waiting for a specific request.
- Prioritization:
    - Allows clients to prioritize requests, enabling more important resources to be loaded first.
- Cumulative Acknowledgment:
    - Uses cumulative acknowledgment for streams, which can improve performance in certain scenarios.

3. HTTP/3
- Connection Model:
    - Based on QUIC (Quick UDP Internet Connections), a transport layer network protocol that uses UDP instead of TCP, which allows for faster connection establishment and improved performance.
- No Head-of-Line Blocking:
    - Eliminates head-of-line blocking entirely at the transport layer because QUIC streams operate independently, allowing for true multiplexing.
- Faster Connection Establishment:
    - Offers faster connection establishment due to 0-RTT (zero round-trip time) connection resume, enabling quicker load times for returning users.
- Improved Security:
    - Integrated TLS 1.3 for improved security and performance, simplifying the security model by incorporating encryption directly into the transport layer.
- Stream Management:
    - Each stream can be prioritized independently, and QUIC supports better congestion control mechanisms.
- Resilience to Loss:
    - QUIC is designed to recover from packet loss without affecting other streams, resulting in more reliable performance in lossy environments.

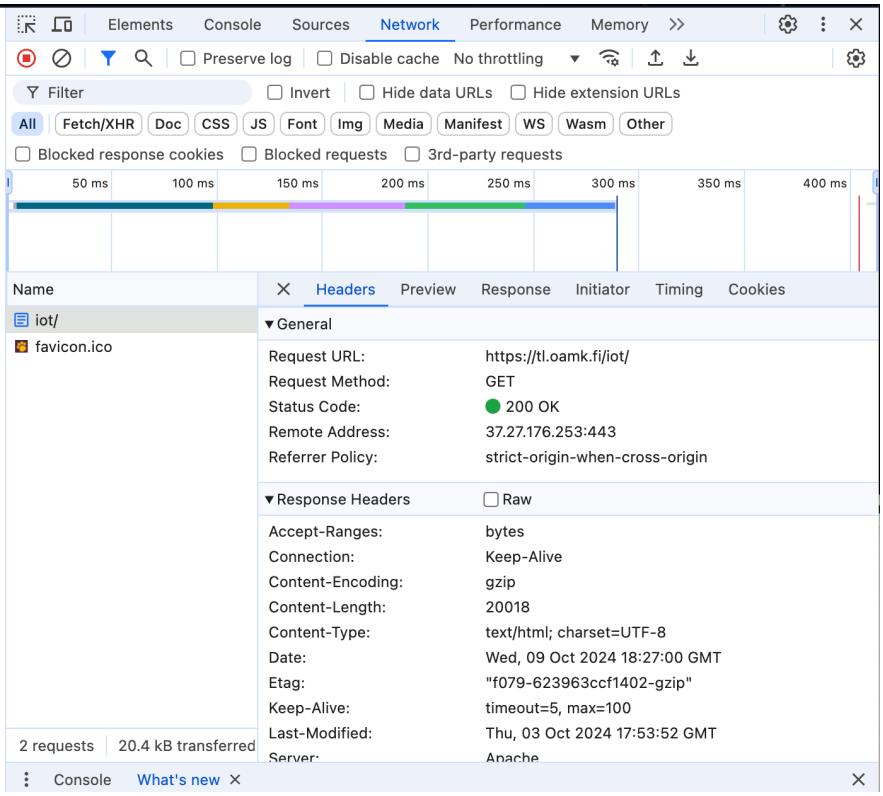
Question 50: Use Chrome or other Chromium based browser and it's developer tools (F12), and access the course web page tl.oamk.fi/iot/. From the developer tools network tab, select the main page: iot/ and check the response headers. Answer:

- What is the connection type?
- What is the server software the web server announced?
- Was any compression / encoding being used? (content-encoding)
- Is there X-Xss-Protection set in the response?
- Is there Strict-Transport-Security set in the response?

Answer 50:

protocols like TCP/IP, data formats such as JSON and XML, and security systems like (PKI/HTTPS) won't usually work at all or are not very optimal to be used in resource limited wireless sensor networks (low power and lossy networks)?

48. What is the MTU challenge for IPv4 and IPv6 over common wireless low power and lossy wireless connections (Hint: Research Zigbee/IEEE 802.15.4 and Bluetooth MTU vs IPv4 or IPv6)?
49. Compare and list few HTTP/1.1, HTTP/2 and HTTP/3 differencies and features
50. Use Chrome or other Chromium based browser and it's developer tools (F12), and access the course web page tl.oamk.fi/iot/. From the developer tools network tab, select the main page: iot/ and check the response headers. Answer:
    - What is the connection type?
    - What is the server software the web server announced?
    - Was any compression / encoding being used?



Question 51: What is Head-of-Line blocking challenge/problem?

Answer 51: Head-of-Line (HoL) blocking is a performance issue that occurs in networking and communication protocols, primarily in connection-oriented transport protocols like TCP (Transmission Control Protocol). This challenge arises when multiple packets are queued for transmission or processing, and the first packet must be fully processed before subsequent packets can be processed or transmitted Head-of-Line blocking is a significant challenge in traditional connection-oriented protocols like TCP, where the processing of packets can be delayed due to the queuing of packets. This leads to increased latency and reduced throughput, especially in networks with high delay or packet loss. Modern protocols like HTTP/2 and HTTP/3, along with techniques like multiplexing and using UDP, are designed to mitigate the effects of HoL blocking, leading to better performance and user experience in various applications.

Question 52: What is reverse proxy. List some advantages and features?

Answer 52: Reverse Proxy

A reverse proxy server acts as a gateway, intercepting requests from clients and forwarding them to the appropriate backend servers. It can be used to improve performance, security, and load balancing in web applications.

Advantages:

- Improved performance: By caching frequently accessed content and optimizing requests, a reverse proxy can significantly improve the performance of web applications.
- Enhanced security: A reverse proxy can help protect backend servers from attacks by acting as a firewall and filtering malicious traffic.
- Load balancing: Reverse proxies can distribute traffic across multiple backend servers, ensuring that no single server becomes overloaded.
- Simplified management: A reverse proxy can centralize management tasks, making it easier to configure, monitor, and maintain web applications.
- SSL termination: A reverse proxy can handle SSL/TLS encryption, offloading this computationally expensive task from backend servers.

Features:

- Caching: Caches frequently accessed content to reduce latency and improve performance.
- Load balancing: Distributes traffic across multiple backend servers to improve scalability and availability.
- SSL termination: Handles SSL/TLS encryption, providing a secure connection between clients and the reverse proxy.
- Compression: Compresses content to reduce bandwidth usage and improve performance.
- Security: Provides security features such as firewalling, intrusion detection, and rate limiting.
- Web application firewall (WAF): Protects against common web application attacks like SQL injection and cross-site scripting.
- CDN integration: Can be integrated with a content delivery network (CDN) to further improve performance and global reach.

Question 53: What is Web application firewall (WAF). List some advantages and features?

Answer 53: A Web Application Firewall (WAF) is a security device or software that sits between a web server and the internet, acting as a filter for incoming HTTP requests. It inspects incoming traffic for malicious patterns and attacks, protecting web applications from various threats.

Advantages:

- Protection against web application attacks: WAFs can detect and block common web application attacks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and session hijacking.
- Centralized security management: WAFs provide a centralized point for managing and monitoring security policies, reducing the burden on individual web application developers and administrators.
- Improved performance: By offloading security tasks from web application servers, WAFs can improve overall application performance.
- Enhanced compliance: WAFs can help organizations comply with industry regulations and standards, such as PCI DSS and HIPAA.
- Reduced risk of data breaches: By preventing web application attacks, WAFs can help reduce the risk of data breaches and financial losses.

Features:

- Rule-based inspection: WAFs use rules to define malicious patterns and behaviors, allowing for flexible customization and fine-grained control.
- Signature-based detection: WAFs can detect known attacks by comparing incoming traffic to a database of attack signatures.
- Anomaly detection: WAFs can identify unusual or suspicious behavior that may indicate an attack.
- Bot management: WAFs can help manage bot traffic, preventing malicious bots from attacking web applications.
- Integration with other security tools: WAFs can be integrated with other security tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) systems.
- Cloud-based deployment: WAFs can be deployed as a cloud-based service, providing scalability and ease of management.

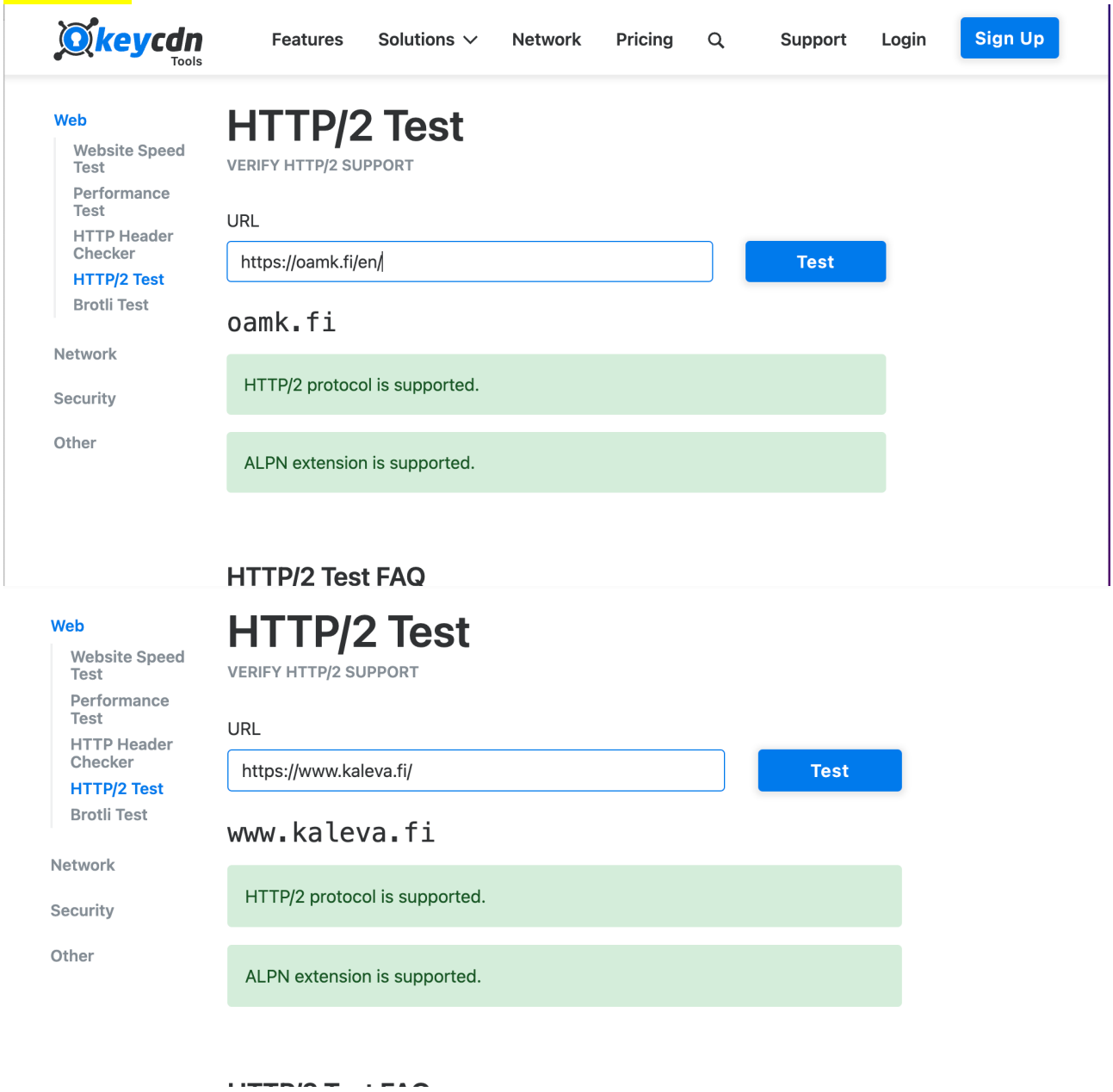
Question 54: What are Websockets?

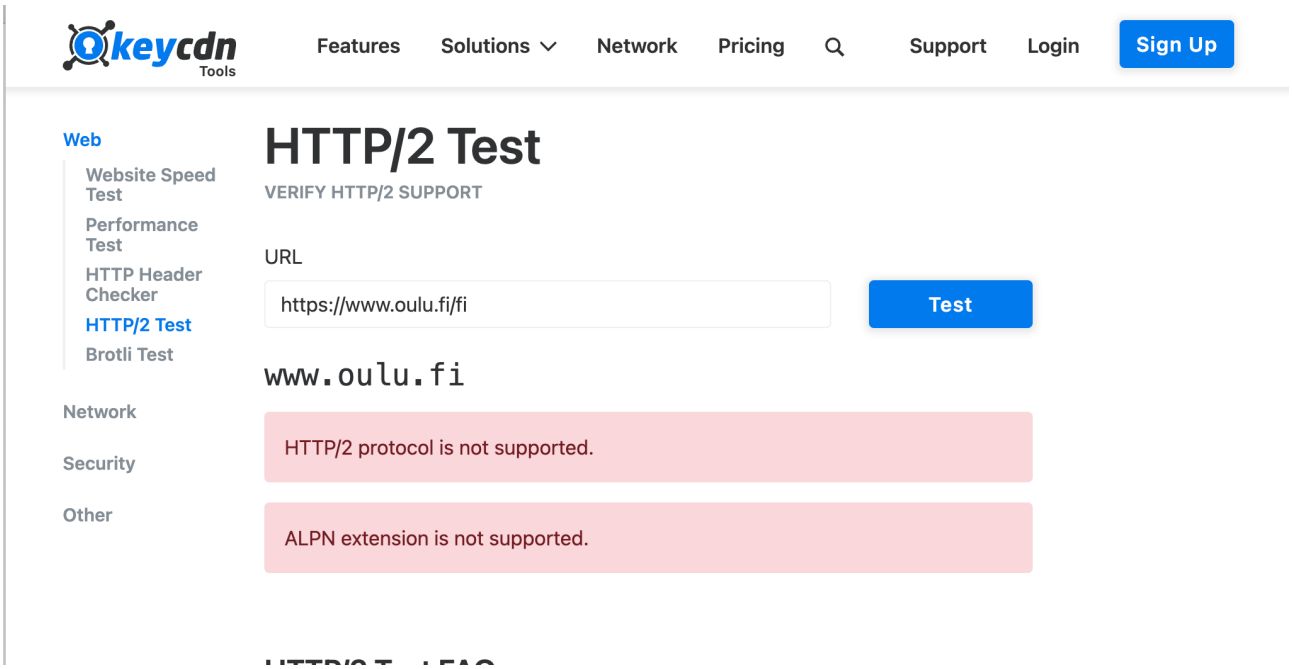
Answer 54: A WebSocket is a communication protocol that provides full-duplex communication channels over a single TCP connection. It enables real-time, event-driven connection between a client and a server.
Unlike traditional HTTP software, which follows a request-response model, WebSockets allow two-way (bi-directional) communication. This means that the client and the server can send data to each other anytime without continuous polling. WebSockets are used for real-time, event-driven communication between clients and servers. They are essential for applications needing instant updates, such as real-time chat, messaging, and multiplayer games.
In traditional HTTP, clients continuously poll the server, causing increased latency and inefficiency. WebSockets, however, establish a persistent connection, allowing data to flow both ways instantly without repeated requests. This enables seamless real-time communication, enhancing user experience.
For example, in a chat application, messages can be delivered instantly to all users without refreshing the page or frequent HTTP requests. WebSockets support bi-directional communication, allowing servers to push updates to clients, fostering more interactive applications.
Google Chrome was the first browser to include standard support for WebSockets in 2009. RFC 6455—The WebSocket Protocol—was officially published online in 2011. The Google WebSocket Protocol and WebSocket API are standardized by the W3C and the IETF, and support across browsers is very common.

Question 55:What is HTTP Long Polling?
Answer 55: HTTP Long Polling is a technique used to push information to a client as soon as possible on the server. As a result, the server does not have to wait for the client to send a request. In Long Polling, the server does not close the connection once it receives a request from the client. Instead, the server responds only if any new message is available or if a timeout threshold is reached.
Once the client receives a response, it immediately sends a new request to the server to have a new pending connection to send data to the client, and the operation is repeated. With this approach, the server emulates a Realtime Server Push feature. HTTP Long polling is a mechanism where the server can send data independently or push data to the client without the web client making a request. The information is then pushed as it becomes available, which makes it real-time. However, it works best if the messages from the server are rare and not too frequent.

Question 56: Use this tool to check few websites whether the server supports HTTP/2: tools.keycdn.com/http2-test. Two examples: www.kaleva.fi and www.oulu.fi

Answer 56:


keycdn Tools
Features
Solutions
Network
Pricing
Support
Login
Sign Up
Web
Website Speed Test
Performance Test
HTTP Header Checker
HTTP/2 Test
Brotli Test
Network
Security
Other
HTTP/2 Test
VERIFY HTTP/2 SUPPORT
URL
https://oamk.fi/en/
Test
oamk.fi
HTTP/2 protocol is supported.
ALPN extension is supported.
HTTP/2 Test FAQ
Web
Website Speed Test
Performance Test
HTTP Header Checker
HTTP/2 Test
Brotli Test
Network
Security
Other
HTTP/2 Test
VERIFY HTTP/2 SUPPORT
URL
https://www.kaleva.fi/
Test
www.kaleva.fi
HTTP/2 protocol is supported.
ALPN extension is supported.



Question57. Study Google Firebase documentation and advertisements. Think and list examples how to use Firebase ecosystem with Android application(s) or with some IoT other system?

Answer 57: Firebase is a robust platform that offers a suite of tools for building, improving, and growing mobile and web applications. Its seamless integration and powerful features make it an ideal choice for Android app development and IoT integration. This guide will explore some key use cases and best practices for leveraging Firebase in these domains.

Android App Development

1. Authentication:
    - User Management: Implement secure authentication methods like email/password, Google Sign-In, Facebook Login, and more.
    - Password Recovery: Provide a user-friendly process for resetting forgotten passwords.
    - Custom Claims: Store additional user information and control access to specific features using custom claims.
2. Real-time Database and Cloud Firestore:
    - Data Synchronization: Store and synchronize data in real-time across multiple devices.
    - Collaborative Applications: Build applications where users can work on the same data simultaneously.
    - IoT Integration: Store sensor data, device states, and other IoT-related information.
3. Cloud Storage:
    - File Storage: Store user-generated content like images, videos, and documents.
    - File Sharing: Implement features for sharing files with other users.
    - File Management: Provide tools for organizing and managing stored files.
4. Crashlytics:
    - Crash Reporting: Monitor and diagnose app crashes to improve stability.
    - Performance Monitoring: Track app performance metrics to identify bottlenecks and optimize user experience.

…

Week 7

Question 59: Describe shortly following security tools/terms/concepts:

- CVE
- CVSS
- Asymmetric encryption
- Symmetric encryption
- Disassembler
- Overflow vulnerability
- Race condition vulnerability
- ASLR/DEP/NX
- Ghidra
- RCE vulnerability
- Local privilege escalation
- Zero-day vulnerability
- Zero-click exploit
- SQL injection
- Command injection vulnerability
- Cross-site scripting
- Information disclosure
- Code deobfuscation / obfuscation
- OSINT
- Data exfiltration
- Lateral movement
- Command & Control
- Social engineering
- IDS/NIDS
- SIEM

Answer 59: Short description is given below:-
Common Vulnerabilities and Exposures (CVE): A publicly accessible database of known vulnerabilities in software and hardware.

Common Vulnerability Scoring System (CVSS): A standardized framework for assessing the severity of vulnerabilities.
Asymmetric Encryption: A cryptographic algorithm that uses a pair of keys (public and private) for encryption and decryption.
Symmetric Encryption: A cryptographic algorithm that uses the same key for both encryption and decryption.
Disassembler: A tool that converts machine code into assembly language.
Buffer Overflow: A vulnerability that occurs when a program attempts to write more data to a fixed-size buffer than it can hold, potentially leading to code execution.
Race Condition: A timing-based vulnerability that arises when the order of operations can affect the outcome of a program.
Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), and Non-Executable (NX): Security mechanisms used to prevent certain types of attacks, such as buffer overflows and code injection.
Ghidra: A free and open-source reverse engineering suite.
Remote Code Execution (RCE): A vulnerability that allows an attacker to execute arbitrary code on a remote system.

Local Privilege Escalation: A vulnerability that allows an attacker to gain elevated privileges on a system they already have access to.
Zero-Day Vulnerability: A vulnerability that is unknown to the vendor and has no patch available.
Zero-Click Exploit: An attack that can compromise a system without requiring any user interaction.
SQL Injection: A vulnerability that allows an attacker to inject malicious SQL code into a web application.
Command Injection: A vulnerability that allows an attacker to inject malicious commands into a web application.
Cross-Site Scripting (XSS): A vulnerability that allows an attacker to inject malicious scripts into a web page.
Information Disclosure: A vulnerability that allows an attacker to access sensitive information.
Code Deobfuscation/Obfuscation: Techniques used to make code more or less readable.
Open-Source Intelligence (OSINT): Information gathered from publicly available sources.
Data Exfiltration: The unauthorized transfer of data from a system.
Lateral Movement: An attacker's ability to move from one compromised system to another within a network.
Command and Control (C&C): A server used by attackers to communicate with compromised systems.
Social Engineering: Manipulating people to gain unauthorized access or information.
Intrusion Detection System (IDS)/Network Intrusion Detection System (NIDS): A system that detects and alerts on suspicious activity.
Security Information and Event Management (SIEM): A software platform that collects, analyzes, and correlates security data.

Question 60: Explain Microsoft's STRIDE threat model shortly (see the old software vulnerability slides)

Answer 60: Microsoft's STRIDE threat model is a framework designed to identify and categorize security threats in software systems. It helps developers and security professionals systematically assess the vulnerabilities in an application and the potential risks associated with them. STRIDE is an acronym where each letter represents a different type of threat:

S – Spoofing Identity Refers to attacks where an attacker pretends to be someone else by using false credentials or identity.

T – Tampering with Data Involves malicious modification of data while in transit or storage, compromising the integrity of the system.

R – Repudiation Refers to the inability to prove an action was performed by a user, allowing the user to deny having performed it (e.g., denying a transaction or an action in a system).

I – Information Disclosure Occurs when sensitive data is exposed to unauthorized parties, leading to privacy or confidentiality breaches.

D – Denial of Service (DoS) Involves attacks that disrupt the normal functioning of services, making resources unavailable to legitimate users.

E – Elevation of Privilege Refers to scenarios where an attacker gains unauthorized access to elevated privileges or roles, such as administrative access.

STRIDE helps to address these types of threats during the design phase, enabling teams to build more secure systems by proactively recognizing and mitigating vulnerabilities.

Question 61: Explain Microsoft's DREAD risk model shortly (see the old software vulnerability slides)

Answer 61: The DREAD risk model is a framework created by Microsoft for assessing and prioritizing security threats by assigning scores to various risk factors. It helps quantify the severity of potential security issues so that developers can determine the risks that need to be addressed first. DREAD is an acronym that stands for the following five factors:

D – Damage Potential : Measures the potential impact of the threat. How much damage could the exploit cause if it were successful? For example, does it crash the system, steal data, or affect many users?

R – Reproducibility : Evaluates how easily the threat can be replicated. Can the attack be performed reliably and repeatedly by anyone, or is it complex and unlikely to occur?

E – Exploitability : Looks at how easy or difficult it is to exploit the vulnerability. Does it require advanced skills or special equipment, or can it be exploited with simple tools?

A – Affected Users : Considers the number of users affected by the vulnerability. Does the threat impact a large portion of the user base or just a small, isolated group?

D – Discoverability : Assesses how easily the vulnerability can be discovered. Is the flaw obvious to attackers, or would it take advanced techniques or insider knowledge to find?

Each factor is scored, typically on a scale from 1 to 10, and the total score helps prioritize which threats require immediate attention. The DREAD model assists in both risk management and threat mitigation by offering a systematic way to evaluate potential security vulnerabilities.

This model is often used alongside other threat modeling techniques like STRIDE to improve overall software security.

Question 62: Check some CVEs of widely used applications from https://www.cvedetails.com/ and answer:

- Describe what is the CVE scoring system
- When was the last time when Exim (MTA, mail transfer agent, more modern version of the application, not the Cambridge version) had a critical vulnerability? What is the CVE number?
- Describe CVE-2016-6210 vulnerability shortly. Optional: How can you prevent such attack / vulnerability?
- Describe CVE-2019-15846 vulnerability shortly
- Describe CWE-208 from https://cwe.mitre.org/data/archive.html (download most recent PDF)

Answer 62: CVE-2024-39929 is a critical remote code execution vulnerability that affects Exim, a widely used mail transfer agent (MTA). This vulnerability allows an attacker to send a specially

crafted email to an Exim server and execute arbitrary code on the system. If exploited, this vulnerability could allow an attacker to gain complete control over the Exim server, including the ability to read, modify, or delete sensitive information. This could lead to significant data breaches, service disruptions, and other serious consequences. Exim has released a patch to address this vulnerability. It is strongly recommended that all Exim users apply the patch as soon as possible.
The CVSS score is based on three main metrics:

- Base: This metric reflects the inherent characteristics of the vulnerability, such as the ease of exploitation and the potential impact on confidentiality, integrity, and availability.
- Temporal: This metric considers the availability of patches, exploits, and other factors that can change the severity of the vulnerability over time.
- Environmental: This metric reflects how the vulnerability could affect a specific environment, such as the type of data that is at risk or the security controls that are in place.

The CVSS score can be used to help organizations prioritize their vulnerability remediation efforts. Vulnerabilities with a higher CVSS score are more likely to be exploited and should be addressed first.

Question 63: Study D-Link DNS-320 ShareCenter write-up in the ExploitDB

- What kind of software exploit is that?
- Try to explain shortly (summarise) from the write-up, how the attacker can elevate access to become root (administrator) user?

Answer 63:
The D-Link DNS-320 ShareCenter exploit found on ExploitDB allows an attacker to elevate their privileges and potentially gain root (administrator) access through command injection vulnerabilities in the NAS device's web interface.
This specific exploit occurs within the device's administrative interface. The vulnerable module, /cgi/login_mgr.cgi, contains a parameter called “port” that can be manipulated. An attacker, without needing authentication, can inject arbitrary commands into this parameter. These commands are then executed with root privileges on the system, allowing the attacker to take full control of the device. This can lead to access to all files stored on the device and potentially other network-connected systems.
To prevent such an attack, users are advised to ensure their firmware is up to date and to follow best security practices like disabling any unnecessary network services and using strong authentication mechanisms. Disabling remote administration access when not required can also mitigate risks

Question 64: Read this short article about cracking SIM cards and answer these questions:

- What is “side-channel attack”?
- How side-channel attack was used to crack SIM cards?

Answer 64: A side-channel attack is a type of cryptographic attack that exploits physical signals emitted by a device during computation. These signals can reveal information about the secret keys or data being processed. Common side-channel signals include:

- Power consumption: The amount of power a device consumes can vary depending on the operations being performed.
- Electromagnetic radiation: Devices emit electromagnetic radiation as a byproduct of their operations.
- Timing: The amount of time it takes a device to perform certain operations can vary depending on the data being processed.

Researchers have successfully used side-channel attacks to crack the encryption on SIM cards. By analyzing the power consumption or electromagnetic radiation emitted by a SIM card during cryptographic operations, attackers can extract information about the secret key used to encrypt

and decrypt data. This type of attack is particularly effective against SIM cards because they are relatively small and have limited power supplies. As a result, it is easier to measure their physical signals and extract sensitive information.

Question 65: Browse this public penetration test report and news article and answer these questions:

- Penetration test report has header *security through obscurity* (next to the item 171 and onwards). What does it mean?
- Penetration test report items 114 - 141 describe remote attack and vulnerability. What kind of problem is it?

Answer 65:

Security Through Obscurity:

"Security through obscurity" refers to relying on secrecy or hiding system details as the primary method of securing software or networks. In a penetration testing context, this practice is viewed as inadequate because once the obscurity is bypassed (e.g., by reverse-engineering or gathering information), the system is vulnerable. Instead, security should be based on strong, well-tested cryptography and protocols, not just on hiding the implementation details.

Remote Attack :

The vulnerability described between items 114-141 in the penetration test report is likely related to improper handling of remote access controls, exposing the system to external attacks. This could involve vulnerabilities like command injection, improper authentication mechanisms, or an exploitable service, enabling attackers to perform remote code execution or gain unauthorized access. Such flaws could allow attackers to compromise sensitive data or take control of systems remotely.

Question 66: Read this news article about garage door security vulnerability and answer:

- What information security and privacy issues were found and listed in the article?
- What was the main issue and vulnerability with MQTT configuration/architecture?
- Read the CVE-2023-1748 (it's about this vulnerability). How much (i.e. how bad) is the base CVSS score? What is the CWE code for this kind of vulnerability?

Answer 66: The article discusses a significant security and privacy issue involving Nexx Smart Home devices, which allow for remote control of garage doors and smart plugs. The main vulnerability lies in the use of hard-coded credentials, a serious flaw where attackers can gain unauthorized access to the MQTT server, thereby controlling any Nexx customer's devices remotely.

The vulnerability, identified as CVE-2023-1748, has a CVSS base score of 10.0, which indicates a critical severity. This score reflects the ease with which an attacker can exploit this vulnerability,

given that it requires no user interaction, can be executed remotely over the network, and compromises confidentiality, integrity, and availability.

In terms of the architectural flaw with MQTT, the core issue is that Nexx's devices expose these hard-coded credentials in a way that attackers can access and exploit them, allowing unauthorized control of the devices. The CWE code for this vulnerability is CWE-798, which pertains to the use of hard-coded credentials, a common and critical issue in embedded and IoT devices.

Question 67: Browse this "Secure development - towards approval" PDF document from National Cyber Security Centre Finland and answer from TESTING AND VERIFICATION chapter:

- What is unit testing?
- What is component testing?
- What is system testing?
- What is acceptance testing?
- What is static testing?
- What is dynamic testing?
- What is fuzzing?

Answer 67:

Unit Testing: This process focuses on individual components of the software, ensuring that each small part (like functions or methods) works as intended in isolation.

Component Testing: This phase involves testing entire modules or components to validate their functionality and interactions with other components.

System Testing: Conducted on the fully integrated system, this testing verifies that all components function together correctly and meet overall specifications.

Acceptance Testing: This final phase evaluates whether the system satisfies user requirements and is ready for deployment, ensuring it meets business or client needs.

Static Testing: This method reviews the code or documentation without executing it, aiming to identify potential defects early in the development lifecycle through techniques like code reviews and inspections.

Dynamic Testing: In contrast to static testing, this involves executing the code in a runtime environment to observe its behavior and performance under various conditions, ensuring it operates correctly.

Fuzzing: This technique involves feeding random or unexpected data into the system to uncover security vulnerabilities and stability issues, helping to identify weaknesses that could be exploited.

Question 68: Browse this "Instructions – Supply chain attack" PDF document from National Cyber Security Centre Finland and research/answer:

- What is supply chain attack?
- What is 3-2-1 backup rule?
- What is network segmentation and how/why it improves information security?

Answer 68:

Supply Chain Attack: A cyberattack that targets vulnerabilities within an organization's supply chain, often by compromising third-party vendors or software to infiltrate the primary organization's network.

3-2-1 Backup Rule: A strategy recommending that you maintain three copies of your data, stored on two different types of media, with one copy kept offsite. This approach ensures data availability and protection against data loss.

Network Segmentation: Dividing a computer network into smaller segments to improve security. It restricts lateral movement within the network, minimizing the potential damage from a breach and enhancing monitoring and control over sensitive data.

Question 69: Check some recent vulnerabilities being exploited in the wild from cisa.gov. Select one, summarise the problem, and search and study some news articles about the vulnerability

Answer 69: One of the recent vulnerabilities identified by the Cybersecurity and Infrastructure Security Agency (CISA) is CVE-2023-22515, a critical flaw in Atlassian Confluence. This vulnerability allows unauthenticated remote attackers to create unauthorized administrator accounts on Confluence servers, enabling them to gain full control over the instance.

Exploit Mechanism: Attackers can exploit this vulnerability by making a request to the unauthenticated /server-info.action endpoint. This action alters the server's configuration, misleading it to think the setup process is incomplete, which then allows the attacker to access the /setup/setupadministrator.action endpoint and create a new administrator account.

Impact: Once an attacker has administrative privileges, they can modify settings, exfiltrate data, or potentially deploy malicious software within the system

Risk Level: CISA and the FBI classify this vulnerability as a significant threat, particularly because it has been actively exploited in the wild, prompting the agency to add it to their Known Exploited Vulnerabilities Catalog.

…

Week 8

Question 1: Nnnn
Answer 1: Nnnn

Question 2: Nnnn
Answer 2: Nnnn

Question 3: Nnnn
Answer 3: Nnnn

Question 4: Nnnn
Answer 4: Nnnn

…