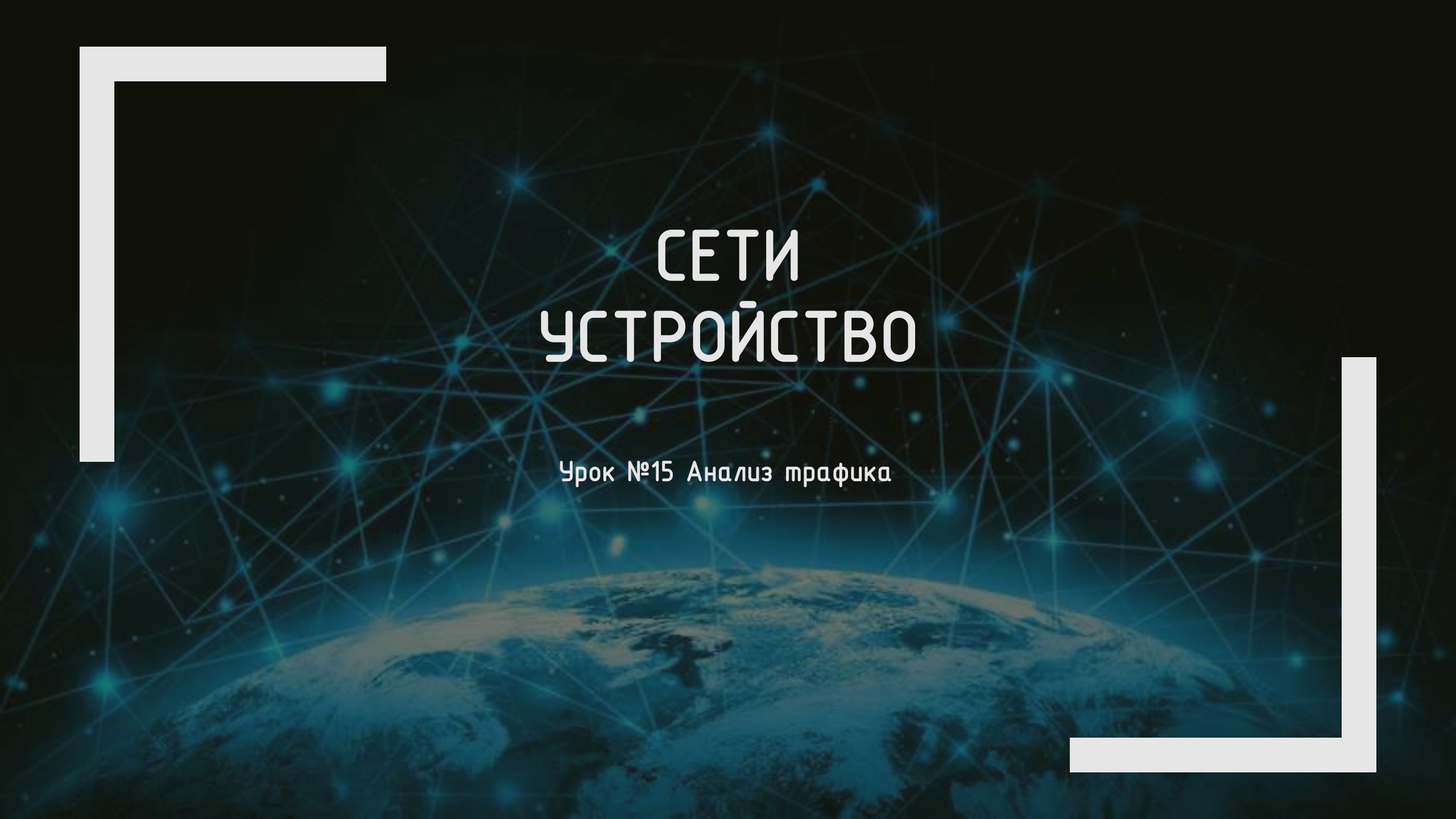
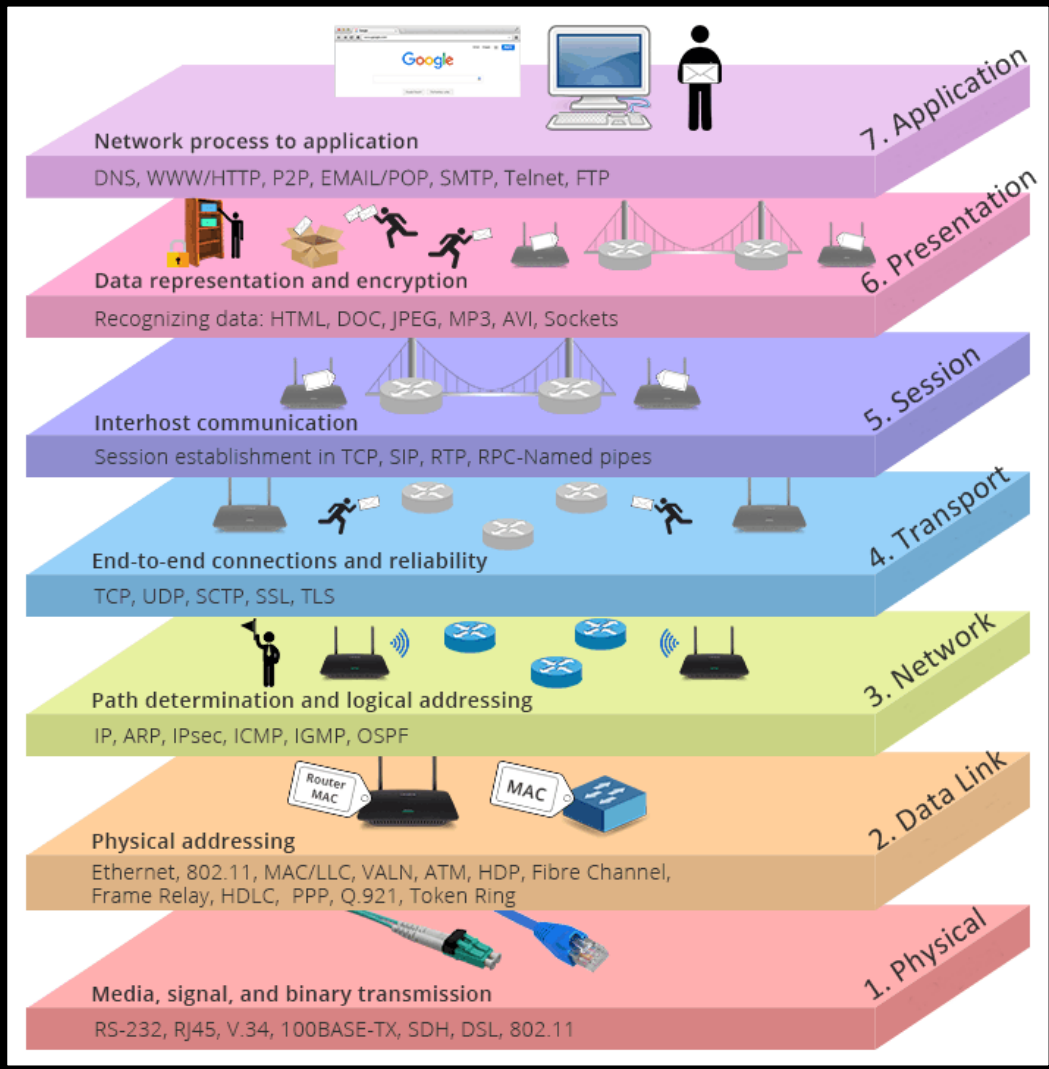


СЕТИ
УСТРОЙСТВО

Урок №15 Анализ трафика

Актуализация

OSI


Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

OSI

Три имени компьютера

Три имени компьютера

MAC – физический адрес. Внутрисетевое общение

08-00-0F-A4-00-3E

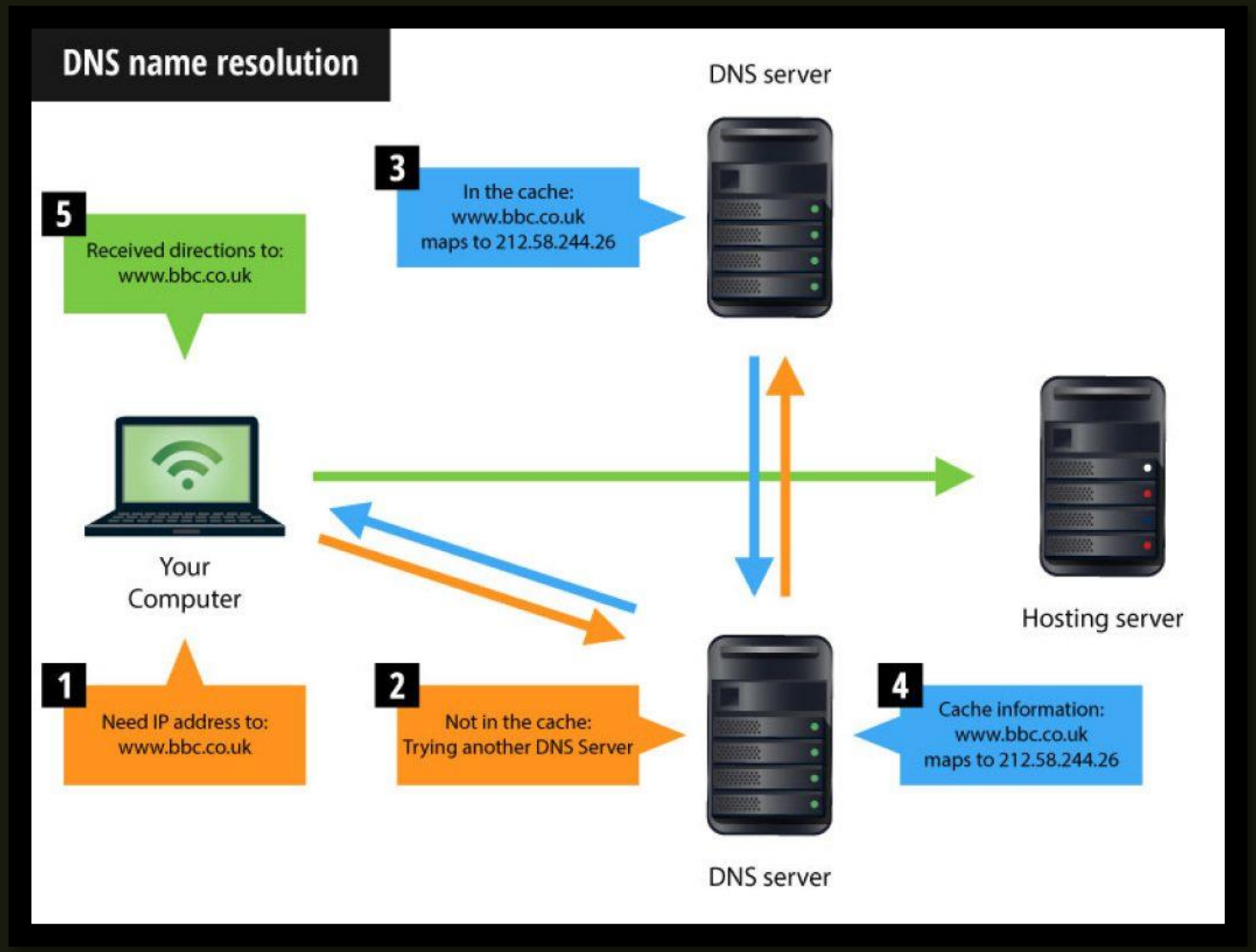
IP – логический адрес. Межсетевое общение

192.168.15.1

NB – NetBios имя. Общение в локальной сети

SeregaCool

DNS


DNS name resolution
DNS server
3
In the cache:
www.bbc.co.uk
maps to 212.58.244.26
5
Received directions to:
www.bbc.co.uk
Your
Computer
Hosting server
1
Need IP address to:
www.bbc.co.uk
2
Not in the cache:
Trying another DNS Server
4
Cache information:
www.bbc.co.uk
maps to 212.58.244.26
DNS server

DNS

Анализ трафика

Сниффинг

Сниффер может анализировать только то, что проходит через его сетевую карту.

Использование коммутаторов и их грамотная конфигурация уже является защитой от прослушивания.

Перехват трафика может осуществляться:

- обычным «прослушиванием» сетевого интерфейса;
- подключением сниффера в разрыв канала;
- ответвлением трафика;
- через анализ побочных электромагнитных излучений и восстановление трафика;
- через атаку, приводящую к перенаправлению трафика жертвы.

Задачи сниффинга

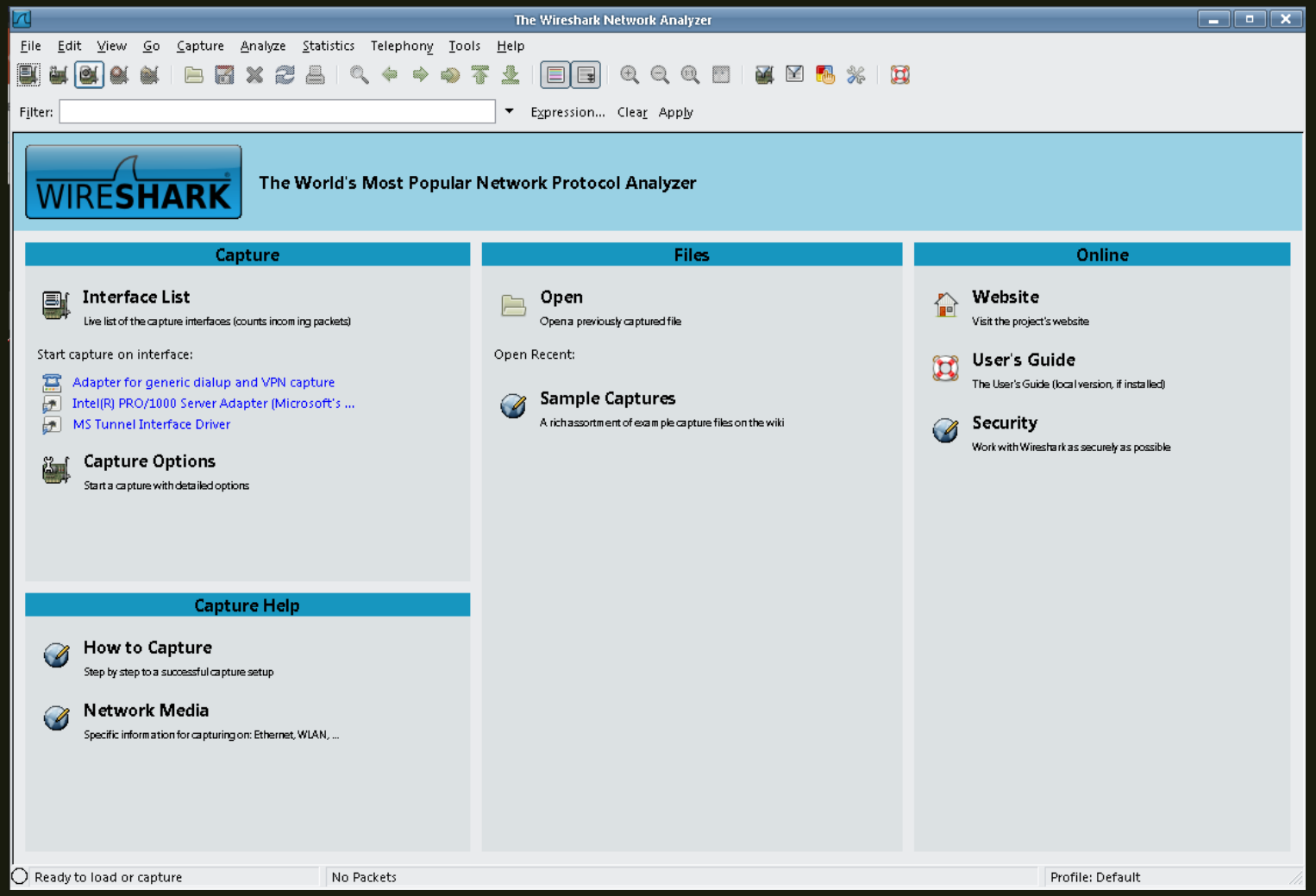
Хорошие:

- Диагностировать работу сети и Локализовать неисправность сети или ошибку конфигурации сетевых агентов
- Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи
- Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие

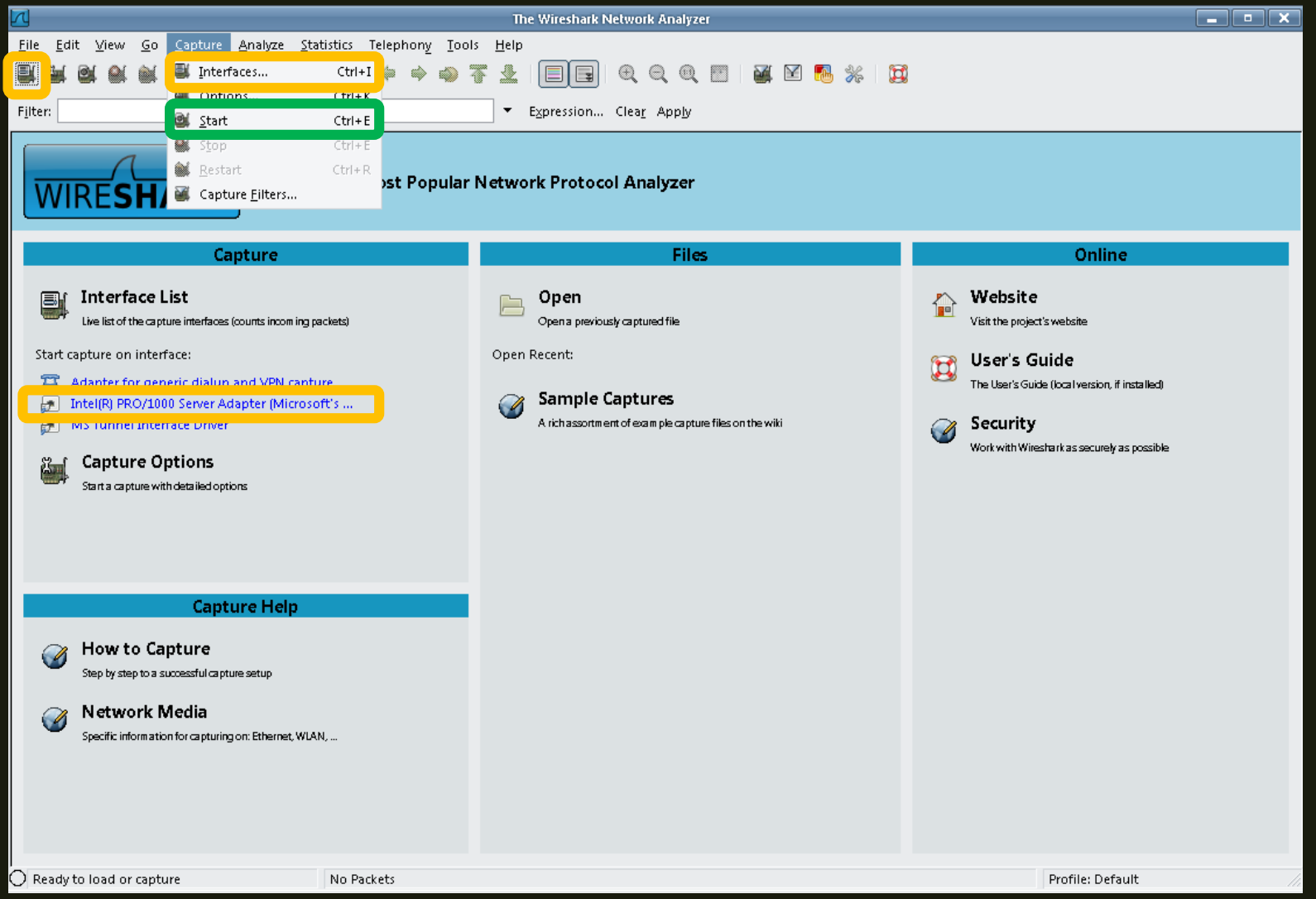
ПО

- WinPcap – расширение драйвера сетевой карты
- Ethereal – сниффер, построенный на основе WinPcap (стабильный)
- Wireshark – сниффер, построенный на основе Ethereal (удобный)

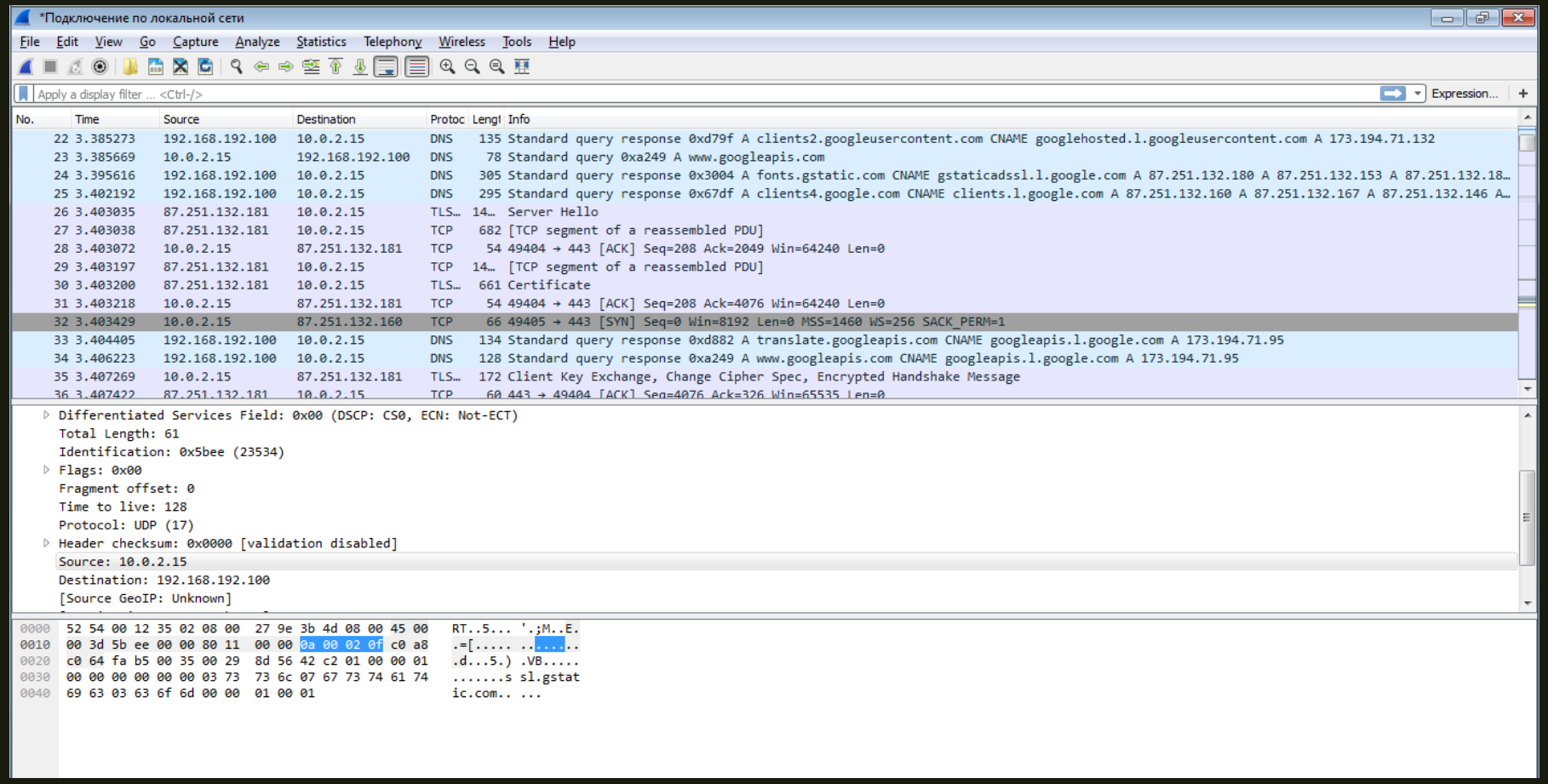
WireShark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Adapter for generic dialup and VPN capture
Intel(R) PRO/1000 Server Adapter (Microsoft's ...
MS Tunnel Interface Driver
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

Выбор интерфейса



Процесс перехвата

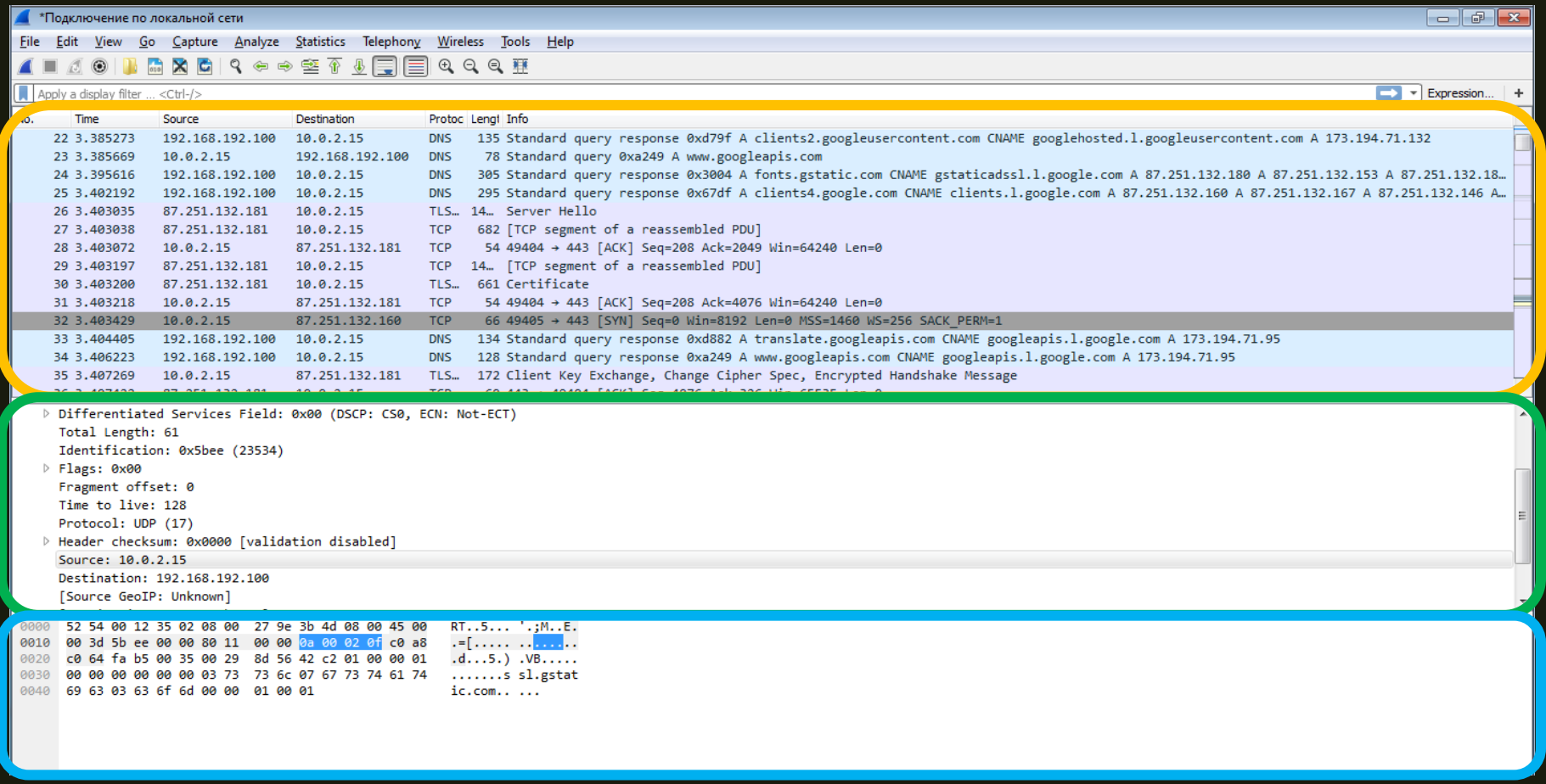


Процесс перехвата

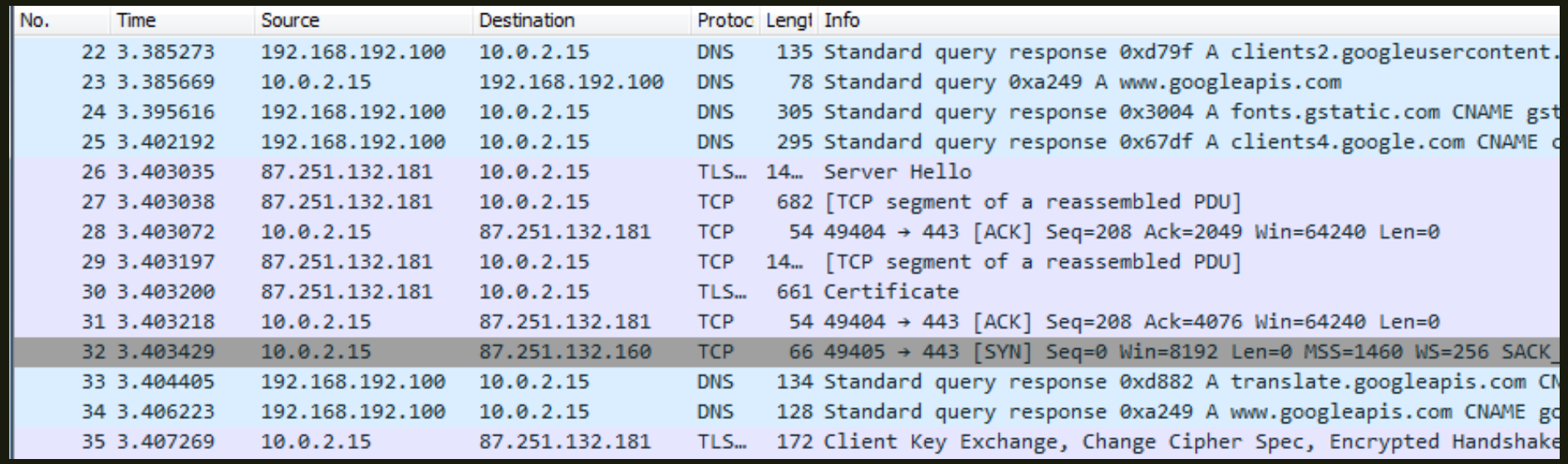
Список пакетов

Расшифровка

Оригинал данных

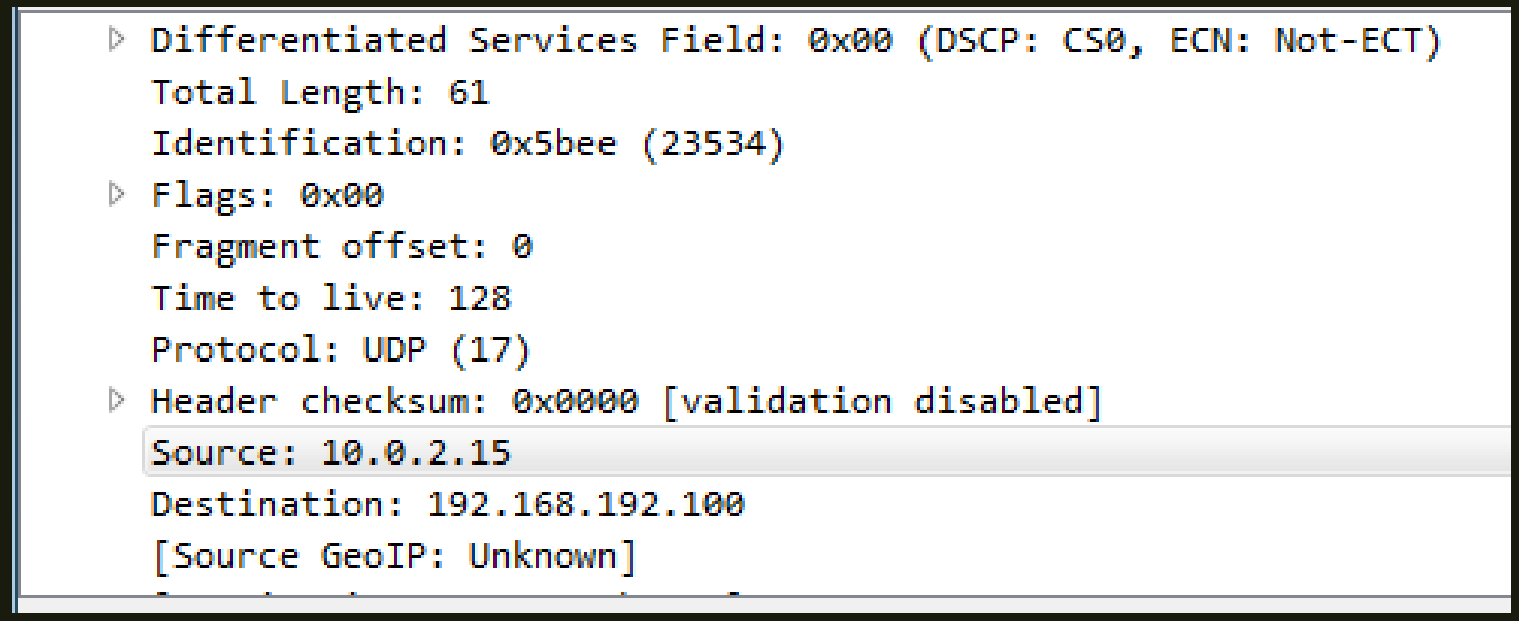


Список пакетов

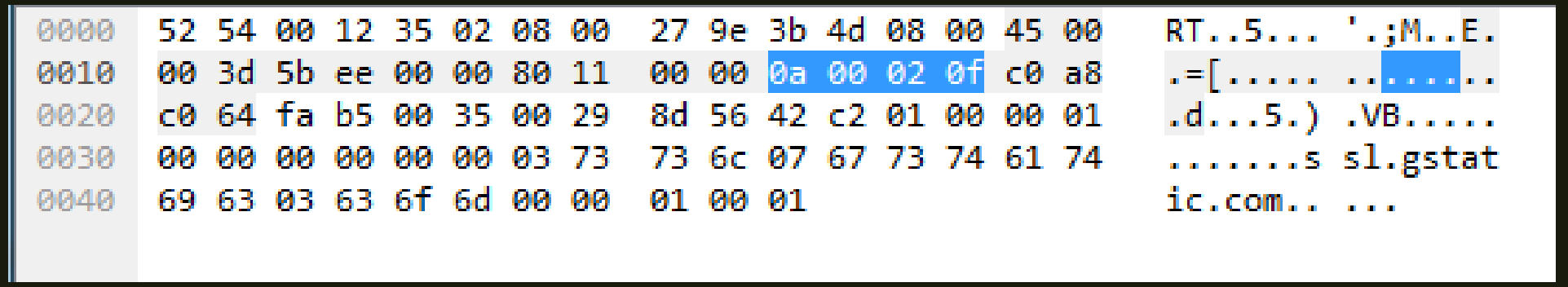


No.	Time	Source	Destination	Protoc	Lengt	Info
22	3.385273	192.168.192.100	10.0.2.15	DNS	135	Standard query response 0xd79f A clients2.googleusercontent.
23	3.385669	10.0.2.15	192.168.192.100	DNS	78	Standard query 0xa249 A www.googleapis.com
24	3.395616	192.168.192.100	10.0.2.15	DNS	305	Standard query response 0x3004 A fonts.gstatic.com CNAME gst
25	3.402192	192.168.192.100	10.0.2.15	DNS	295	Standard query response 0x67df A clients4.google.com CNAME c
26	3.403035	87.251.132.181	10.0.2.15	TLS…	14…	Server Hello
27	3.403038	87.251.132.181	10.0.2.15	TCP	682	[TCP segment of a reassembled PDU]
28	3.403072	10.0.2.15	87.251.132.181	TCP	54	49404 → 443 [ACK] Seq=208 Ack=2049 Win=64240 Len=0
29	3.403197	87.251.132.181	10.0.2.15	TCP	14…	[TCP segment of a reassembled PDU]
30	3.403200	87.251.132.181	10.0.2.15	TLS…	661	Certificate
31	3.403218	10.0.2.15	87.251.132.181	TCP	54	49404 → 443 [ACK] Seq=208 Ack=4076 Win=64240 Len=0
32	3.403429	10.0.2.15	87.251.132.160	TCP	66	49405 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_
33	3.404405	192.168.192.100	10.0.2.15	DNS	134	Standard query response 0xd882 A translate.googleapis.com CN
34	3.406223	192.168.192.100	10.0.2.15	DNS	128	Standard query response 0xa249 A www.googleapis.com CNAME go
35	3.407269	10.0.2.15	87.251.132.181	TLS…	172	Client Key Exchange, Change Cipher Spec, Encrypted Handshake

Расшифровка содержимого



Оригинальное содержимое

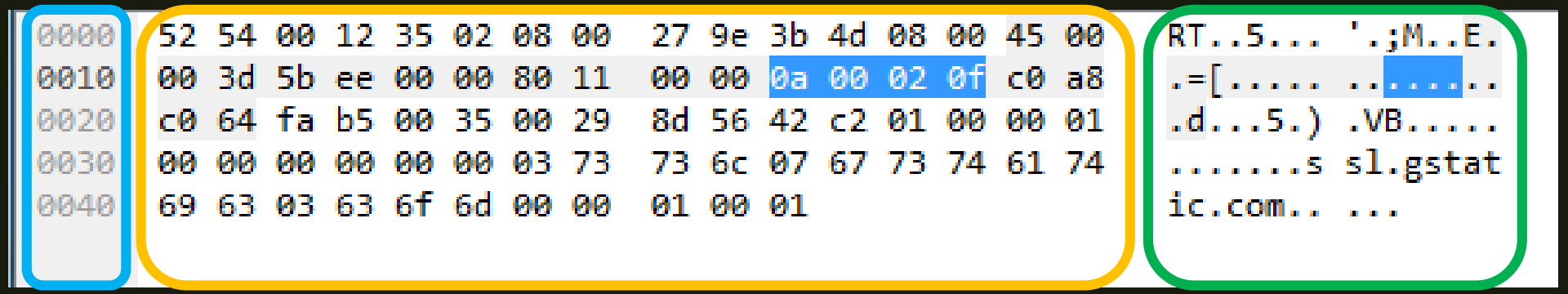


```
0000  52 54 00 12 35 02 08 00  27 9e 3b 4d 08 00 45 00   RT..5... '.;M..E.
0010  00 3d 5b ee 00 00 80 11  00 00 0a 00 02 0f c0 a8   .=[..... ........
0020  c0 64 fa b5 00 35 00 29  8d 56 42 c2 01 00 00 01   .d...5.) .VB.....
0030  00 00 00 00 00 00 03 73  73 6c 07 67 73 74 61 74   .......s sl.gstat
0040  69 63 03 63 6f 6d 00 00  01 00 01                  ic.com.. ...
```

Оригинальное содержимое

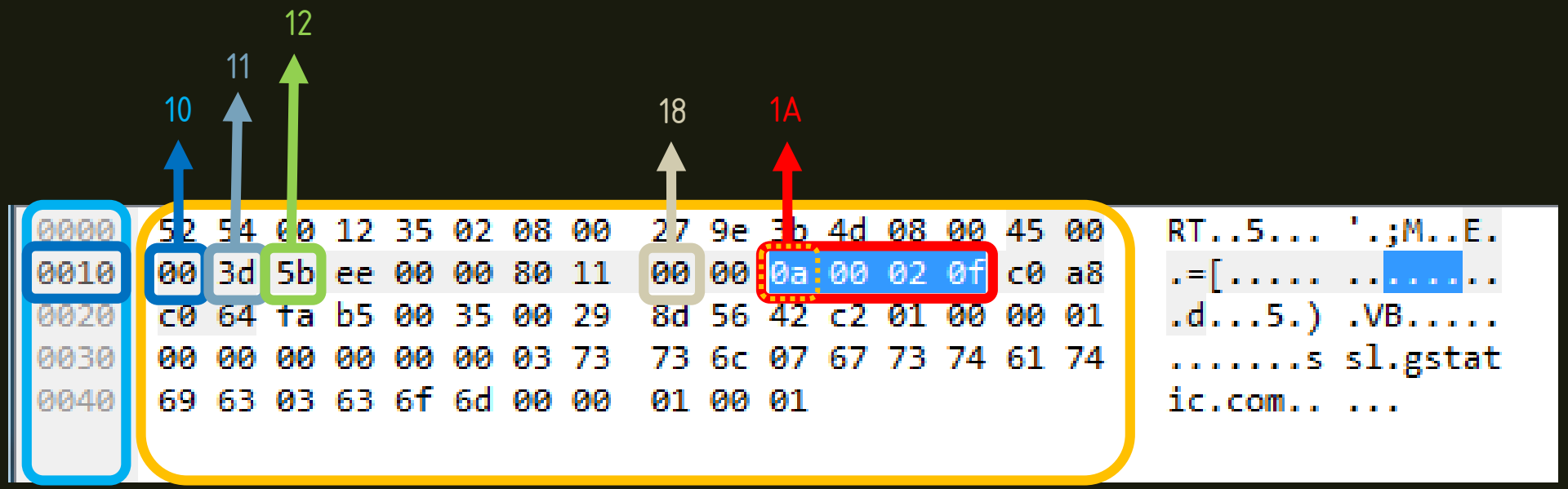
Данные в шестнадцатеричной системе

Перевод по ASCII



Адрес первого байта строки

Адресация


12
11
10
18
1A
0000 52 54 00 12 35 02 08 00 27 9e 3b 4d 08 00 45 00 RT..5... '.;M..E.
0010 00 3d 5b ee 00 00 80 11 00 00 0a 00 02 0f c0 a8 .=[..... ....
0020 c0 64 fa b5 00 35 00 29 8d 56 42 c2 01 00 00 01 .d...5.) .VB.....
0030 00 00 00 00 00 00 03 73 73 6c 07 67 73 74 61 74 ....s sl.gstat
0040 69 63 03 63 6f 6d 00 00 01 00 01 ic.com.. ...

Практика