



廣州軟件學院

SOFTWARE ENGINEERING INSTITUTE OF GUANGZHOU

实验报告封面

课程名称: TCP 和 IP 协议

课程代码: _____

任课老师: _____

实验指导老师: _____

实验报告名称: _____

本实验报告包括以下几个内容:

一、实验目的 ☐

二、实验环境 ☐

三、实验原理 ☐

四、实验步骤 ☐

五、分析与总结 ☐

学生姓名: _____

学号: _____

教学班: _____

递交日期: _____

签收人: _____ (共 页)

我申明,本报告内的实验已按要求完成,报告完全是由我个人完成,并没有抄袭行为。我已经保留了这份实验报告的副本。

申明人(签名): _____

实验报告评语与评分:

评阅老师签名:

一、实验名称： 协议分析软件操作实验

二、实验目的

理解 tcp/ip 协议基本原理，掌握 Wireshark 和科来网络分析系统基本操作

三、实验软硬件环境：

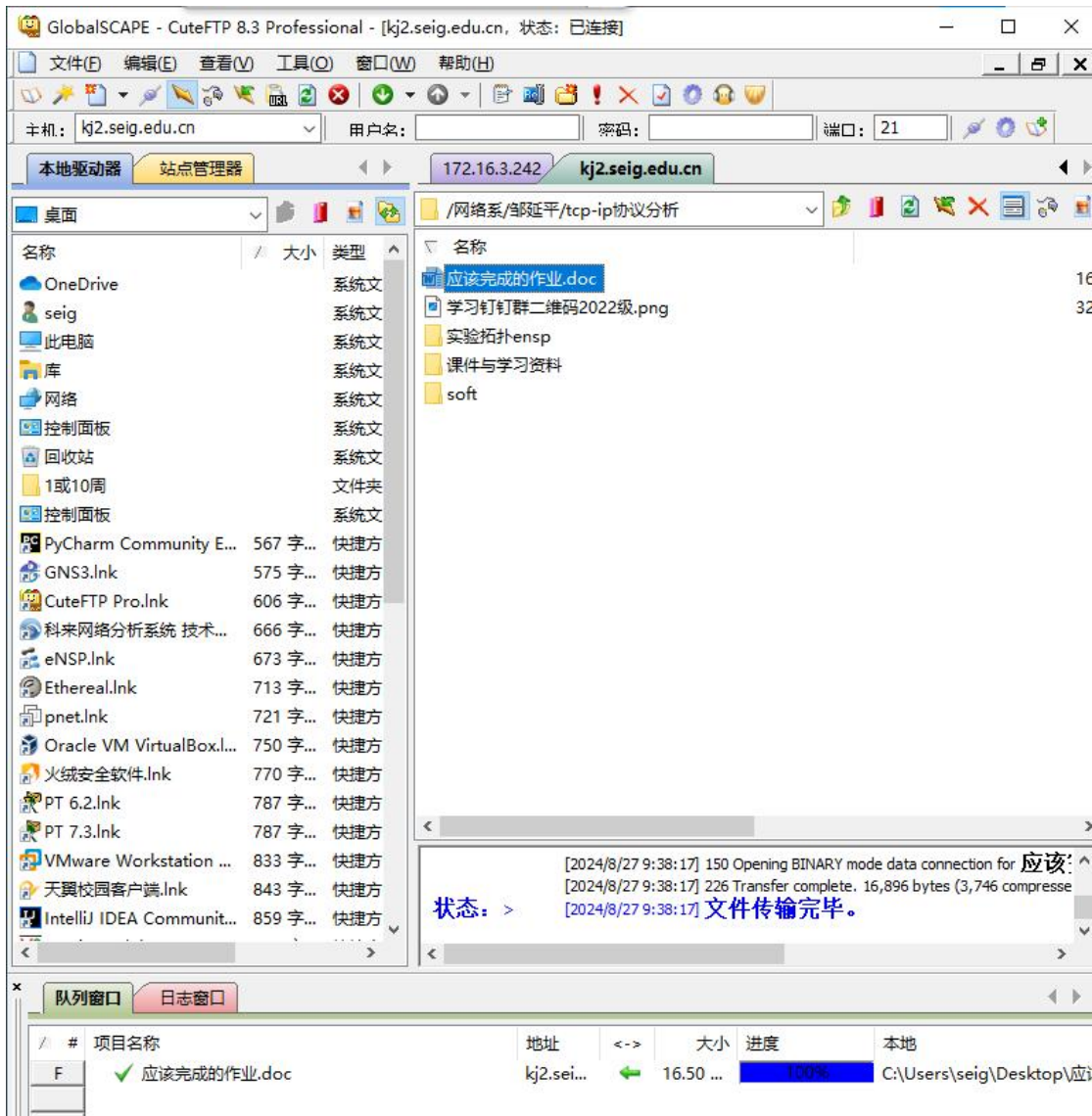
软件系统： Wireshark 和科来网络分析系统

四、实验要求与步骤

学习阅读相关学习材料，完成实验并回答实验问题

访问 <http://www.seig.edu.cn> 和 www.qq.com、my.seig.edu.cn 等，浏览网页，
登陆 <ftp://kj2.seig.edu.cn> 下载文件，进行相应网络操作，运行 Wireshark 软件练习抓包，并将抓包数据文件存盘(cap 格式)，用科来网络分析系统导入文件数据包，完成实验报告并截图，并分析回答相关问题。

1) 登陆 ftp://kj2.seig.edu.cn 下载文件相关数据包截图



ftp.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ftp

表达式...

No.	Time	Source	Destination	Protocol	Length	Info
615	4.913513	172.16.3.242	172.16.54.147	FTP	92	Response: 220 S
616	4.915531	172.16.54.147	172.16.3.242	FTP	63	Request: USER K
631	5.045519	172.16.3.242	172.16.54.147	FTP	90	Response: 331 U
632	5.045930	172.16.54.147	172.16.3.242	FTP	63	Request: PASS K
642	5.162576	172.16.3.242	172.16.54.147	FTP	84	Response: 230 U
643	5.163777	172.16.54.147	172.16.3.242	FTP	59	Request: PWD
653	5.271972	172.16.3.242	172.16.54.147	FTP	85	Response: 257 "
654	5.272418	172.16.54.147	172.16.3.242	FTP	60	Request: FEAT
671	5.380219	172.16.3.242	172.16.54.147	FTP	766	Response: 211-E
672	5.382308	172.16.54.147	172.16.3.242	FTP	62	Request: MODE Z
680	5.495264	172.16.3.242	172.16.54.147	FTP	70	Response: 200 M
681	5.495561	172.16.54.147	172.16.3.242	FTP	62	Request: REST 0
693	5.585469	172.16.3.242	172.16.54.147	FTP	100	Response: 350 F
694	5.586039	172.16.54.147	172.16.3.242	FTP	60	Request: PASV
725	5.822731	172.16.3.242	172.16.54.147	FTP	104	Response: 227 E
726	5.823249	172.16.54.147	172.16.3.242	FTP	60	Request: LIST
741	5.946409	172.16.3.242	172.16.54.147	FTP	107	Response: 150 C
773	6.247607	172.16.3.242	172.16.54.147	FTP	171	Response: 226 T
911	7.065834	172.16.54.147	172.16.3.242	FTP	67	Request: CWD /\
924	7.214813	172.16.3.242	172.16.54.147	FTP	88	Response: 250 C
926	7.215282	172.16.54.147	172.16.3.242	FTP	60	Request: PASV
951	7.521304	172.16.3.242	172.16.54.147	FTP	104	Response: 227 E

> Frame 615: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: HuaweiTe_74:25:ae (60:f1:8a:74:25:ae), Dst: 18:c0:4d:1b:f6:17 (18:c0:4d:1b:f6:17)
> Internet Protocol Version 4, Src: 172.16.3.242, Dst: 172.16.54.147
> Transmission Control Protocol, Src Port: 21, Dst Port: 50320, Seq: 1, Ack: 1, Len: 38
> File Transfer Protocol (FTP)
[Current working directory:]

0000	18 c0 4d 1b f6 17 60 f1 8a 74 25 ae 08 00 45 00	..M...`..t%...E.
0010	00 4e 56 a2 40 00 7c 06 15 62 ac 10 03 f2 ac 10	.NV.@. ..b.....
0020	36 93 00 15 c4 90 da 7c 2b d1 06 61 df 23 50 18	6..... +..a.#P.
0030	01 00 cf 72 00 00 32 32 30 20 53 65 72 76 2d 55	...r..22 0 Serv-U
0040	20 46 54 50 20 53 65 72 76 65 72 20 76 31 35 2e	FTP Ser ver v15.
0050	30 20 72 65 61 64 79 2e 2e 2e 0d 0a	0 ready.

已准备好加载或捕获 | 分组: 15843 · 已显示: 60 (0.4%) · 已丢弃: 0 (0.0%) | 配置: Default


2) 访问 <http://www.seig.edu.cn> 相关数据包截图

PNETLab | Topo | 校园新闻 - MYSE | 广州软件学院


https://www.seig.edu.cn

导入书签... 火狐官方网站 新手上路 常用网址 京东商城 移动设备上的书签

您必须先登录此网络才能访问互联网。 打开网络登录页面



廣州軟件學院
SOFTWARE ENGINEERING INSTITUTE OF GUANGZHOU



http

No.	Time	Source	Destination	Protocol	Length	Info
137	1.976619	172.16.54.147	14.116.245.29	HTTP	250	GET /msdownload/update/v3/static/trusted/en/pinrulesst1.cab?6d7584d2a8f46f67 HTTP/1.1
277	3.551230	172.16.54.147	172.16.2.4	HTTP	531	GET / HTTP/1.1
279	3.559355	172.16.2.4	172.16.54.147	HTTP	421	HTTP/1.1 301 Moved Permanently (text/html)
6271	18.902370	172.16.54.147	23.62.46.207	HTTP	165	GET /connecttest.txt HTTP/1.1
6272	18.902752	23.62.46.207	172.16.54.147	HTTP	363	HTTP/1.1 302 Found
6345	19.158863	172.16.54.147	23.62.46.207	HTTP	165	GET /connecttest.txt HTTP/1.1
6346	19.159060	23.62.46.207	172.16.54.147	HTTP	363	HTTP/1.1 302 Found

数据包: 172.163.100 - 172.16.54.147 - 分析工程 3

编号	日期	源时间	源	源端口	源地理位置	目标	目标端口	目标地理位置	协议	应用	大小	实际负载	进程
8422	2024/08/27	09:52:33.203740000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP		66	0	
8423	2024/08/27	09:52:33.203752000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP		66	0	
8424	2024/08/27	09:52:33.206971000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	TCP		66	0	
8425	2024/08/27	09:52:33.207071000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP		54	0	
8426	2024/08/27	09:52:33.207080000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP		54	0	
8427	2024/08/27	09:52:33.207635000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	1,514	1,460	
8428	2024/08/27	09:52:33.207635000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	318	264	
8429	2024/08/27	09:52:33.207648000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	1,514	1,460	
8430	2024/08/27	09:52:33.207661000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	318	264	
8431	2024/08/27	09:52:33.211194000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	TCP	Encrypted traffic	60	6	
8475	2024/08/27	09:52:33.223140000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	HTTPS	Encrypted traffic	1,514	1,460	
8476	2024/08/27	09:52:33.234242000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	HTTPS	Encrypted traffic	1,514	1,460	
8477	2024/08/27	09:52:33.234242000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	HTTPS	Encrypted traffic	1,230	1,176	
8478	2024/08/27	09:52:33.234242000	my.seig.educn	443	本地	d83c0aad-1bad-43...	52389	本地	HTTPS	Encrypted traffic	114	60	
8479	2024/08/27	09:52:33.234385000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP	Encrypted traffic	54	0	
8480	2024/08/27	09:52:33.234432000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	TCP	Encrypted traffic	54	0	
8489	2024/08/27	09:52:33.237018000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	147	93	
8490	2024/08/27	09:52:33.237035000	d83c0aad-1bad-4313-b05e-36...	52389	本地	my.seig.educn	443	本地	HTTPS	Encrypted traffic	147	93	

数据包信息(Packet Info)

8426

54

54

2024/08/27 09:52:33.207080000

[0/14]

目的地址(Destination Address)

60:f1:8a:74:25:ae (HUAWEI TECHNOLOGIES CO., LTD

源地址(Source Address)

18:c0:4d:1b:f6:17 (GIGA-BYTE TECHNOLOGY CO., LTD

协议(Protocol Type)

0x0000 (IP) [12/13]

互连网段(Internet Protocol)

版本(Version)

4 [14/1] 0xF0

头部长度(Internet Header Length)

5 (20) [14/1] 0x0F

区分服务字段(Differentiated Services Field)

[15/1]

区分服务码点(Differentiated Services Codepoint)

0000 00.. (默认) [15/1] 0xF0

显示拥塞通告(Explicit Congestion Notification)

.... .00 (不带ECN的传输) [15/1] 0

总长度(Total Length)

40 [16/2]

标识(Identification)

0xcac9 (51961) [18/21]

2240233148web.cap pcapng l.pcapng

文件(F) 编辑(E) 视图(V) 刷新(R) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip.addr == 172.16.54.147 and ip.addr == 172.16.2.4

No.	Time	Source	Destination	Protocol	Length	Info
3771	51.138948	172.16.54.147	172.16.2.4	TCP	66	52351 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3772	51.138957	172.16.54.147	172.16.2.4	TCP	66	[TCP Out-Of-Order] 52351 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3773	51.139652	172.16.2.4	172.16.54.147	TCP	66	80 → 52351 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3774	51.139722	172.16.54.147	172.16.2.4	TCP	54	52351 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
3775	51.139722	172.16.54.147	172.16.2.4	TCP	54	[TCP Dup ACK 3774#1] 52351 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
3843	51.162648	172.16.54.147	172.16.2.4	TCP	66	52352 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3844	51.162653	172.16.54.147	172.16.2.4	TCP	66	[TCP Out-Of-Order] 52352 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3845	51.163865	172.16.2.4	172.16.54.147	TCP	66	80 → 52352 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3846	51.163952	172.16.54.147	172.16.2.4	TCP	54	52352 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
3847	51.163963	172.16.54.147	172.16.2.4	TCP	54	[TCP Dup ACK 3846#1] 52352 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4149	54.383428	172.16.54.147	172.16.2.4	TCP	66	52356 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4150	54.383435	172.16.54.147	172.16.2.4	TCP	66	[TCP Out-Of-Order] 52356 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4151	54.384859	172.16.2.4	172.16.54.147	TCP	66	443 → 52356 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
4152	54.384157	172.16.54.147	172.16.2.4	TCP	54	52356 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4153	54.384163	172.16.54.147	172.16.2.4	TCP	54	[TCP Dup ACK 4152#1] 52356 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
4154	54.384456	172.16.54.147	172.16.2.4	TCP	1514	52356 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=1460 [TCP segment of a reassembled PDU]
4155	54.384456	172.16.54.147	172.16.2.4	TLSv1.2	415	Client Hello
4156	54.384464	172.16.54.147	172.16.2.4	TCP	1514	[TCP Out-Of-Order] 52356 → 443 [ACK] Seq=1 Ack=1 Win=2102272 Len=1460
4157	54.384467	172.16.54.147	172.16.2.4	TCP	415	[TCP Retransmission] 52356 → 443 [PSH, ACK] Seq=1461 Ack=1 Win=2102272 Len=361
4158	54.385364	172.16.2.4	172.16.54.147	TCP	60	443 → 52356 [ACK] Seq=1 Ack=1461 Win=64128 Len=0
4159	54.385364	172.16.2.4	172.16.54.147	TCP	60	443 → 52356 [ACK] Seq=1 Ack=1822 Win=63872 Len=0
4160	54.388208	172.16.2.4	172.16.54.147	TLSv1.2	1514	Server Hello
4161	54.388208	172.16.2.4	172.16.54.147	TCP	1514	443 → 52356 [ACK] Seq=1461 Ack=1822 Win=64128 Len=1460 [TCP segment of a reassembled PDU]

> Frame 3771: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: 18:c0:4d:1b:f6:17 (18:c0:4d:1b:f6:17), Dst: HuaweiTe74:25:ae (60:f1:8a:74:25:ae)

> Internet Protocol Version 4, Src: 172.16.54.147, Dst: 172.16.2.4

> Transmission Control Protocol, Src Port: 52351, Dst Port: 80, Seq: 0, Len: 0

0000 60 f1 8a 74 25 ae 18 c0 4d 1b f6 17 00 00 45 00 ..t....M....E..

0010 00 34 7f ee 40 00 80 06 00 00 ac 10 36 93 ac 10 .4.@....6....

0020 02 04 cc 7f 00 50 0d 8f 72 a6 00 00 00 00 80 02P.....

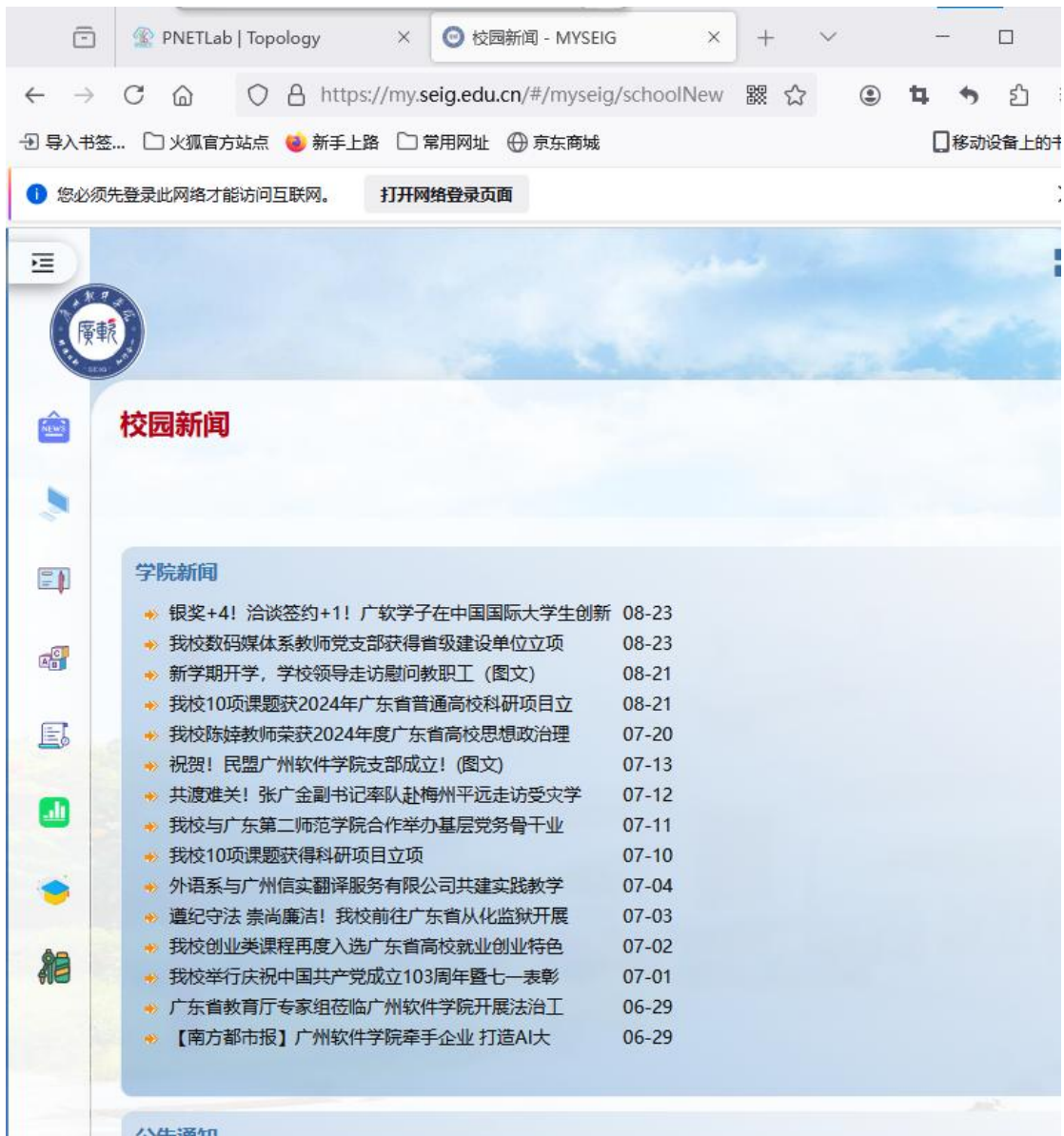
0030 fa f0 90 de 00 00 02 04 05 b4 01 03 03 00 01 01P.....

0040 04 02 ..

2240233148web.cap pcapng l.pcapng

分组: 29027 · 已显示: 210 (0.7%) · 已丢弃: 0 (0.0%) · 配置: default

3) 访问 [https:// my.seig.edu.cn](https://my.seig.edu.cn) 相关数据包截图



编号	日期	绝对时间	源	源端口	源地理位置	目标	目标端口	目标地理位置	协议	应用	大小	实际负载	进程
3771	2024/08/27	09:52:16.635010000	d83c0aad-18ad-4313-b05e-36...	52351	本地	www.seig.edu.cn	80	本地	TCP		66	0	
3772	2024/08/27	09:52:16.635020000	d83c0aad-18ad-4313-b05e-36...	52351	本地	www.seig.edu.cn	80	本地	TCP		66	0	
3773	2024/08/27	09:52:16.635720000	www.seig.edu.cn	80	本地	d83c0aad-18ad-43...	52351	本地	TCP		66	0	
3774	2024/08/27	09:52:16.635790000	d83c0aad-18ad-4313-b05e-36...	52351	本地	www.seig.edu.cn	80	本地	TCP		54	0	
3775	2024/08/27	09:52:16.635800000	d83c0aad-18ad-4313-b05e-36...	52351	本地	www.seig.edu.cn	80	本地	TCP		54	0	
3843	2024/08/27	09:52:16.658708000	d83c0aad-18ad-4313-b05e-36...	52352	本地	www.seig.edu.cn	80	本地	TCP		66	0	
3844	2024/08/27	09:52:16.658721000	d83c0aad-18ad-4313-b05e-36...	52352	本地	www.seig.edu.cn	80	本地	TCP		66	0	
3845	2024/08/27	09:52:16.659933000	www.seig.edu.cn	80	本地	d83c0aad-18ad-43...	52352	本地	TCP		66	0	
3846	2024/08/27	09:52:16.660200000	d83c0aad-18ad-4313-b05e-36...	52352	本地	www.seig.edu.cn	80	本地	TCP		54	0	
3847	2024/08/27	09:52:16.660031000	d83c0aad-18ad-4313-b05e-36...	52352	本地	www.seig.edu.cn	80	本地	TCP		54	0	
4149	2024/08/27	09:52:19.879496000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	TCP		66	0	
4150	2024/08/27	09:52:19.879503000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	TCP		66	0	
4151	2024/08/27	09:52:19.880127000	www.seig.edu.cn	443	本地	d83c0aad-18ad-43...	52356	本地	TCP		66	0	
4152	2024/08/27	09:52:19.880225000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	TCP		54	0	
4153	2024/08/27	09:52:19.880231000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	TCP		54	0	
4154	2024/08/27	09:52:19.880524000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	HTTPS	Encrypted traffic	1,514	1,460	
4155	2024/08/27	09:52:19.880524000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	HTTPS	Encrypted traffic	415	361	
4156	2024/08/27	09:52:19.880532000	d83c0aad-18ad-4313-b05e-36...	52356	本地	www.seig.edu.cn	443	本地	HTTPS	Encrypted traffic	1,514	1,460	

数据包信息(Packet Info)

序号(Number)

3773

数据长度(Packet Length)

66

捕获长度(Capture Length)

66

时间戳(Timestamp)

2024/08/27 09:52:16.635720000

以太网 II(Ethernet II)

目的地址(Destination Address)

18:C0:4D:18:F6:17 (GIGA-BYTE TECHNOLOGY CO.,

源地址(Source Address)

60:F1:8A:74:25:AE (HUAWEI TECHNOLOGIES CO.,L

协议类型(Protocol Type)

0x800 (IP) [12/2]

互联网协议(Internet Protocol)

版本(Version)

4 [14/1] 0xF0

头部长度(Internet Header Length)

5 (20) [14/1] 0x0F

区分服务字段(Differentiated Services Field)

15 [15/1]

区分服务码点(Differentiated Services Codepoint)

0000 00... (默认) [15/1] 0xFC

显示拥塞通告(Explicit Congestion Notification)

.... 00 (不带ECN的传输) [15/1]

总长度(Total Length)

52 [16/2]

标识(Identification)

0x0 (0) [18/2]

18 C0 4D 18 F6 17 60 F1 8A 74 25 AE 00 00 45 00 34 00 00 40 00 3D 06

AD 8C AC 10 02 04 AC 10 36 93 00 50 CC 7F 00 58 41 E7 8D BF 72 A7 88 12

FA F0 54 13 00 00 02 04 05 04 01 01 04 02 01 03 03 07

.....t.....4...@...
.....6...XA...F...
.....

3) 访问 http:// www.qq.com 相关数据包截图

```

C:\Users\seig>nslookup www.qq.com
服务器: UnKnown
Address: 172.16.2.1

非权威应答:
名称:    ins-r23tsuuf.ias.tencent-cloud.net
Addresses: 240e:97c:2f:1::5c
           240e:97c:2f:2::4c
           121.14.77.201
           121.14.77.221
Aliases: www.qq.com

C:\Users\seig>

```

121.14.77.221 121.14.77.201

(ip.addr == 172.16.54.147 and ip.addr ==121.14.77.221)or(ip.addr == 172.16.54.147and ip.addr ==121.14.77.201)



五、实验思考问题

(可在科来分析系统截图说明)

1) 当前网关的 IP 和 MAC 地址是什么？

网站 www.qq.com 向本机返回数据时，其源 ip 地址、源 mac、目标 IP、目标源 mac 是什么？

能否知道网站 www.qq.com 主机的真实 mac？

2) 列举本机捕获到的前 6 个广播包的源 IP 地址、源 mac 地址、目标 IP 地址、目

标 mac 地址，这些广播包是什么协议数据包？有什么作用？

3)本机的网络平均流量是多少？最多的数据包的大小分布怎样？



节点1->	节点1地理位置->	<- 节点2	<- 节点2地理位置	TCP会话	UDP会话	数据包	字节数	开始发包时间	结束发包时间	网络分析IP会话: 166
172.16.54.59	本地	172.16.54.147	本地	0	4	1,022	194.42 KB	2024/08/27 09:39:28.195163000	2024/08/27 09:42:13.432810000	2
172.16.54.59	本地	224.50.50.42	本地	0	1	330	38.67 KB	2024/08/27 09:39:28.258690000	2024/08/27 09:42:13.479234000	2
172.16.54.59	本地	225.2.2.1	本地	0	1	111	12.36 KB	2024/08/27 09:39:28.287318000	2024/08/27 09:42:13.942193000	2
23.223.246.19	美国 加利福尼亚州...	172.16.54.147	本地	11	0	209	15.90 KB	2024/08/27 09:39:28.381898000	2024/08/27 09:41:58.503825000	2
34.107.221.82	美国 南卡罗来纳州...	172.16.54.147	本地	55	0	2,020	157.74 KB	2024/08/27 09:39:28.427737000	2024/08/27 09:42:10.814045000	2
172.16.54.73	本地	239.255.255.250	本地	0	2	6	1.28 KB	2024/08/27 09:39:28.577819000	2024/08/27 09:41:29.588206000	2
172.16.54.48	本地	239.255.255.250	本地	0	2	6	1.28 KB	2024/08/27 09:39:29.026249000	2024/08/27 09:41:30.018561000	2
13.107.42.16	加拿大 魁北克蒙特...	172.16.54.147	本地	5	0	96	89.16 KB	2024/08/27 09:39:29.157617000	2024/08/27 09:40:57.208646000	1
172.16.54.147	本地	172.16.105.163	本地	1	1	661	45.29 KB	2024/08/27 09:39:29.264544000	2024/08/27 09:42:13.974415000	2
172.16.54.147	本地	www.bing.com	中国 北京, Microsoft...	5	0	63	44.36 KB	2024/08/27 09:39:29.266681000	2024/08/27 09:41:58.659052000	2
47.93.93.253	中国 北京, 阿里云	172.16.54.147	本地	9	0	299	63.63 KB	2024/08/27 09:39:29.405507000	2024/08/27 09:42:11.811855000	2
172.16.54.150	本地	239.255.255.250	本地	0	2	6	1.70 KB	2024/08/27 09:39:29.562562000	2024/08/27 09:41:32.601417000	2
172.16.3.242	本地	172.16.54.147	本地	10	1	239	18.28 KB	2024/08/27 09:39:29.620521000	2024/08/27 09:42:04.236774000	2
slscupdate.micro...	美国 弗吉尼亚州...	172.16.54.147	本地	28	0	534	115.61 KB	2024/08/27 09:39:29.982750000	2024/08/27 09:42:04.007527000	2
142.250.69.206	美国 华盛顿州 西雅...	172.16.54.147	本地	2	0	8	528.00 B	2024/08/27 09:39:31.051974000	2024/08/27 09:39:39.329722000	2

节点1->	端口1->	节点1地理位置->	<- 节点2	<- 端口2	<- 节点2地理位置	协议	传输层协议	数据包	字节数	负载	TCP状态
172.16.54.147	52761	本地	172.16.54.59	4809	本地	UDP	UDP	332	27.56 KB	13.94 KB	
172.16.54.147	52760	本地	172.16.54.59	5512	本地	UDP	UDP	360	40.83 KB	26.07 KB	
172.16.54.147	51415	本地	172.16.54.59	4988	本地	UDP	UDP	158	107.61 KB	101.13 KB	
172.16.54.59	57058	本地	172.16.54.147	4988	本地	UDP	UDP	20	1.64 KB	840.00 B	

4)列举本网中前 3 个流量的最大会话的 IP 地址。

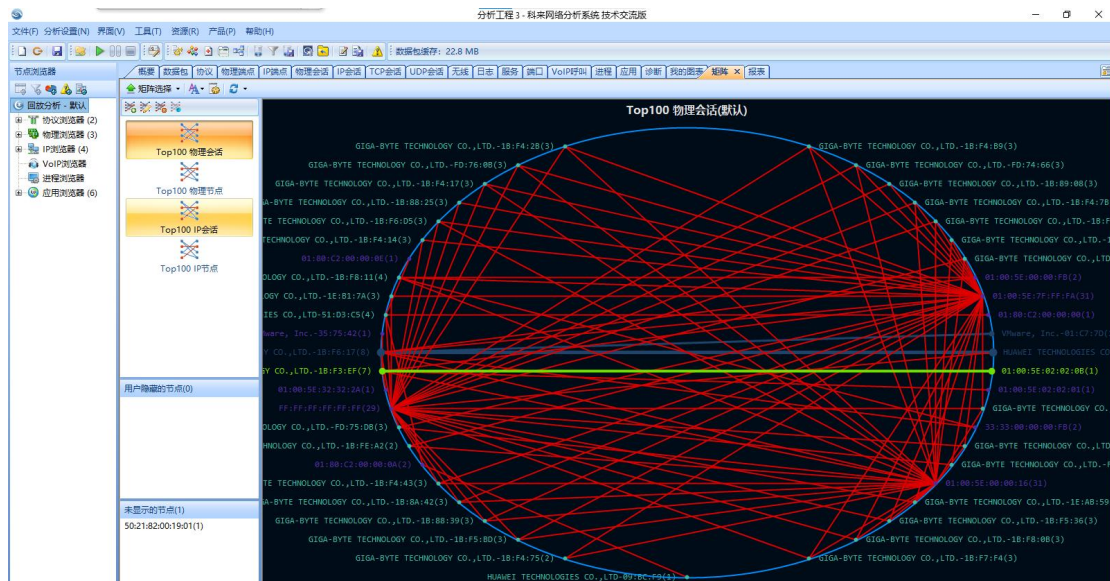
172.16.54.59、172.16.54.113、172.16.54.59



节点1->	节点1地理位置->	<- 节点2	<- 节点2地理位置	TCP会话	UDP会话	数据包	字节数	开始发包时间	结束发包时间	网络分析IP会话: 170
pxui.apic.cn	中国 广东, 东莞, 电信	d83c0aad-18ad-4...	本地	2	0	3,898	3.67 MB	2024/08/27 09:53:18.845345000	2024/08/27 09:53:20.634505000	1
172.16.54.59	本地	225.2.2.1	本地	0	2	2,768	2.37 MB	2024/08/27 09:53:04.468045000	2024/08/27 09:53:24.421307000	1
d83c0aad-18ad-4...	本地	172.16.105.163	本地	1	1	2,335	1.89 MB	2024/08/27 09:51:25.701707000	2024/08/27 09:53:23.494294000	1
ts4.cn.mm.bing.net	中国 湖南, 湘西, 电信	d83c0aad-18ad-4...	本地	6	0	1,433	1.12 MB	2024/08/27 09:52:28.651468000	2024/08/27 09:53:15.052777000	1
staticfile.qq.com	中国 广东, 广州, 电信	d83c0aad-18ad-4...	本地	6	0	1,416	942.35 KB	2024/08/27 09:53:18.842482000	2024/08/27 09:53:20.172842000	1
ltshey.gtmq.com	中国 广东, 广州, 电信	d83c0aad-18ad-4...	本地	1	0	1,406	1.46 MB	2024/08/27 09:53:21.491563000	2024/08/27 09:53:22.495907000	1
ts2.cn.mm.bing.net	中国 浙江, 金华, 电信	d83c0aad-18ad-4...	本地	9	0	1,368	1.16 MB	2024/08/27 09:52:27.784083000	2024/08/27 09:53:18.893561000	1
browser.events.da...	爱尔兰 都柏林, 电信	d83c0aad-18ad-4...	本地	3	0	1,054	1,004.47 KB	2024/08/27 09:52:05.475161000	2024/08/27 09:53:19.248767000	1
assets.msn.cn	中国 江西, 景德镇, 电信	d83c0aad-18ad-4...	本地	2	4	949	465.95 KB	2024/08/27 09:52:05.478769000	2024/08/27 09:53:18.693537000	1
vmvgting.cn	中国 福建, 泉州, 电信	d83c0aad-18ad-4...	本地	1	2	757	600.20 KB	2024/08/27 09:53:19.344307000	2024/08/27 09:53:21.034489000	1
172.16.54.59	本地	172.16.54.113	本地	5	0	745	43.73 KB	2024/08/27 09:51:26.923235000	2024/08/27 09:53:23.221723000	1
172.16.54.59	本地	d83c0aad-18ad-4...	本地	0	4	710	127.89 KB	2024/08/27 09:51:25.685410000	2024/08/27 09:53:24.348420000	1
ntp.msn.cn	中国 江苏, 南通, 电信	d83c0aad-18ad-4...	本地	0	2	708	502.09 KB	2024/08/27 09:52:05.562614000	2024/08/27 09:53:19.991827000	1
d83c0aad-18ad-4...	本地	th.bing.com	中国 北京, Microsoft...	2	0	628	468.08 KB	2024/08/27 09:52:05.557248000	2024/08/27 09:53:18.723051000	1
othve.beacon.qq...	中国 湖南, 长沙, 电信	d83c0aad-18ad-4...	本地	4	2	541	358.64 KB	2024/08/27 09:51:28.806131000	2024/08/27 09:53:22.120639000	1
172.16.54.113	本地	d83c0aad-18ad-4...	本地	23	0	504	108.78 KB	2024/08/27 09:51:52.463736000	2024/08/27 09:53:21.843874000	1
ns1.seig.edu.cn	本地	d83c0aad-18ad-4...	本地	0	147	473	58.17 KB	2024/08/27 09:51:52.461506000	2024/08/27 09:53:23.676546000	1
23.223.246.32	美国 加利福尼亚州...	d83c0aad-18ad-4...	本地	8	0	416	244.39 KB	2024/08/27 09:51:59.325431000	2024/08/27 09:53:19.029334000	1
puuiqpic.cn	中国 广东, 东莞, 电信	d83c0aad-18ad-4...	本地	3	1	397	302.49 KB	2024/08/27 09:53:19.578000000	2024/08/27 09:53:19.639183000	1
appcfv.qq.com	中国 广东, 深圳, 电信	d83c0aad-18ad-4...	本地	2	0	366	160.29 KB	2024/08/27 09:53:19.040666000	2024/08/27 09:53:20.340058000	1
d83c0aad-18ad-4...	本地	erib.msn.cn	中国 北京, Microsoft...	3	0	360	278.66 KB	2024/08/27 09:53:09.477745000	2024/08/27 09:53:18.464633000	1

节点1->	端口1->	节点1地理位置->	<- 节点2	<- 端口2	<- 节点2地理位置	协议	传输层协议	数据包	字节数	负载	TCP状态
d83c0aad-18ad-4313-b05e-366945fcb241locat	52389	本地	my.seig.edu.cn	443	本地	HTTPS	TCP	241	143.28 KB	130.30 KB	ESTABLISHED

5)主视图区中的矩阵有什么作用？



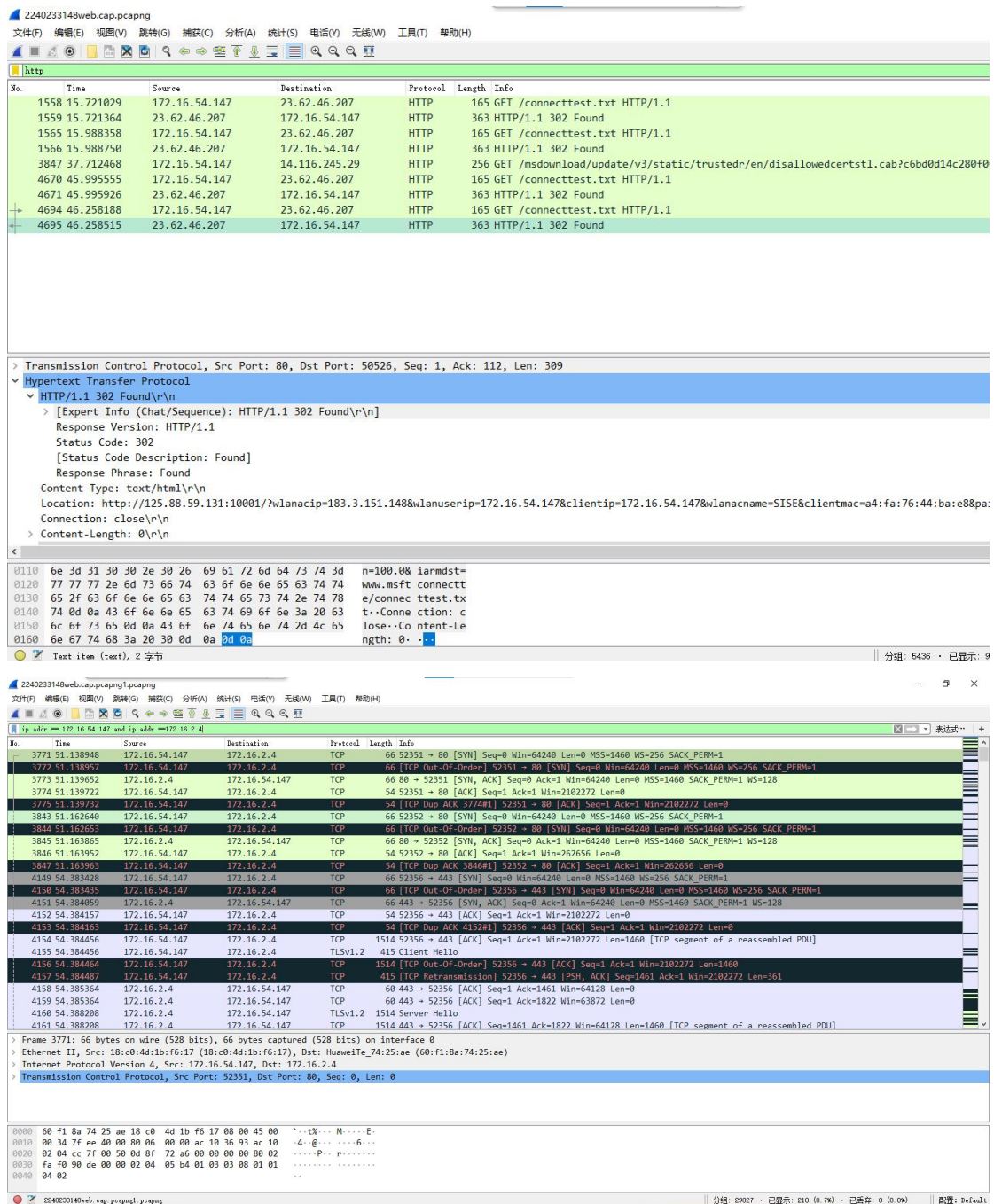
6)当前网络中网络协议有哪些？流量最大是什么？

7)本机只可以捕获到哪些数据包？为什么？

8) 找出本机与网站 **www.seig.edu.cn** 通讯的所有数据包，导出存盘文件(学号+web.cap,不大于 10M)。

(nslookup www.seig.edu.cn)

ip.addr == 172.16.54.147 and ip.addr ==172.16.2.4



9)如何在交换式网络环境中布置科来网络分析系统，以便捕获所有网络节点的数据包？请画拓扑图说明。（重点）-可参考 pnet 平台

10)解释一下 Filter string 表达式的含义：（重点）

①ip.addr == 172.16.2.4 and ip.addr ==172.16.19.155

显示 IP 为 172.16.2.4 和 172. 16.19.155 之间通信的数据包或 IP 源地址或目标地址

为) 172.16.2.4 和 172.16.19.155

②ip.dst==172.16.2.4 || ip.src==172.16.28.10

显示 IP 地址为 172.16.28.10 的发送

IP 目标地址为 172.16.2.4 并且地址为 172.16.19.155

③ip.addr==172.16.39.1 && ! http

④(ip.addr ==172.16.3.240) and (tcp.port ==21)

⑤ip.addr==192.168.10.1 && tcp.port!=80

⑥eth.addr==00.d0.f8.00.00.03

显示 eth 为 MAC 地址为 00.d0.f8.00.00.03

按规范格式写实验报告，附实验数据包截图、认真完成实验问题答案，并导出数据包 **web.cap** 文件，打包压缩上传

注意：

完成相关实验后必须提交实验报告，按时上交，基本要求如下：（以后所有实验报告要求相同）

- 1) 认真填写实验报告封面
- 2) 认真按要求完成相关实验操作，在实验要求和步骤的相关文字处添加自己所完成的实验操作截图，可附文字说明，排版美观
- 3) 必须认真回答实验思考和分析作业问题，问题回答的质量为重要评分依据（分值占比 **50-70%**）