

Digital Forensics & Packet Analysis

UBNetDef, Spring 2022
Week 12

About Me



Education

- ◇ Bachelor of Science, Business Administration
- ◇ Master of Science, MIS



Security Experience

- ◇ Consultant/Senior Consultant, Cyber Risk services, Deloitte
- ◇ Lead Cybersecurity Consultant and vCISO, Loptr LLC



Professional Affiliations

- ◇ ISC²; Certified Information Systems Security Professional (CISSP)
- ◇ Buffalo Electronic Crimes Task Force



Publications:

- ◇ Vulnerability Assessment (ISACA, 2017)



Hats worn:

- | | |
|--------------------|-------------------------------|
| ◇ Virtual CISO | ◇ Security Monitoring Analyst |
| ◇ Project Manager | ◇ Security Architect |
| ◇ Security Analyst | ◇ Software Developer |



Dominic Sellitto, CISSP



Clinical Assistant Professor
Program Director, MS Business Analytics

Skills



Agenda

1. Digital Forensics Overview
2. Subdomains within Digital Forensics
3. Network Forensics Overview
4. Wireshark Exercise 1
5. Wireshark Exercise 2
6. Homework

What is Digital Forensics

- ⬡ Digital Forensics is “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”

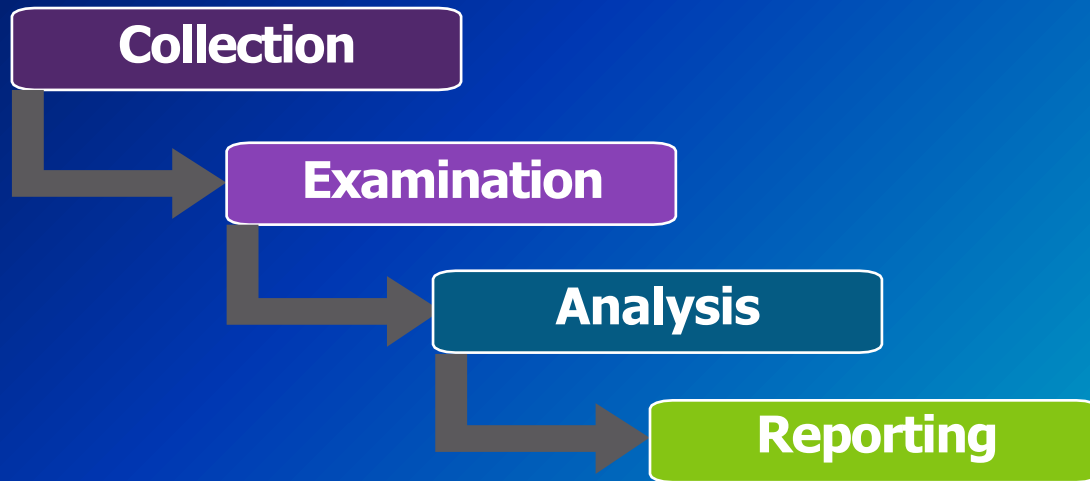
- ⬡ NIST SP-800-86, Guide to Integrating Forensic Techniques Into Incident Response (Pg. 15)

- ⬡ Digital Forensics may also be referred to as:

- ⬡ Computer and Network Forensics
 - ⬡ Data Forensics

Phases of the Forensics Process

- ⬡ **NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response** describes the 4 phases of the forensics process as follows:



Enabling Factors

⬡ In order to repeatedly execute the process, you need some things...

Governance:

- Policies
- Procedures
- Standards

Collection

Finances:

- Tools
- Technologies
- Training

Examination

People

- Investigators
- IT Professionals
- Incident Response Team
- In-house vs. Outsourced

Analysis

Reporting

Location:

- Lab/Room
- Access Control
- Monitoring

Forensic Areas of Practice

⬡ You might just think of forensics as examining hard drives, but it's much more than that:



Media Forensics



Malware Analysis



Memory Forensics



Network Forensics



Mobile Forensics



Cloud Forensics



Email Forensics



Digital Media
Manipulation



IoT Forensics



Automobile
Forensics



Digital Media Manipulation

Which of these is fake?



netdef

Malware Analysis...

- What's that program *really* doing?



Email Forensics...

Greetings,

We are a unique Investment Consultation Firm registered in the United Kingdom; we specialize in searching for potential investments opportunities for our high net-worth clients worldwide. Our aim and motivation is securing a safe and stable investment opportunity for our clients in order to achieve the maximum return on their investments.

We have an investor based here in the United Kingdom currently looking for a profitable project to invest into, any project/proposal that will generate a reasonable and stable return of investment. We have examined your company's profile and consider you to fit our criteria provisionally. We will be glad to partner with you in any viable project initiative within our scope of funding.

We also pay 1% commission to brokers, who introduce project owners for finance or other opportunities. If you think your firm will do better with some extra funding and or business expansion in a partnership or an investment loan; then please email your executive summary/ business plan to us for review and consideration.

Should this be of interest to you, please do not hesitate to e-mail us for further information

Kind regards,

Mr. Floyd W. Brown
Investment accredited broker London - UK.



NetDef

Network Forensics

- ⬡ **Packets** contain all of the information being sent across a network, including the source and destination machine, protocol being used, and the actual data being sent
- ⬡ **Network logs** are records of network events - they tell you that something happened over the network (like source, destination, protocol) but do not contain the actual data that was sent

Network Forensics- Capturing Packets

Packets can be captured using a variety of methods:



Network tap

- ◇ A device placed between two networked devices that captures traffic flowing between



Port Mirroring

- ◇ Sends “copies” of packets flowing through a network switch to a specified location (e.g., packet capture server)

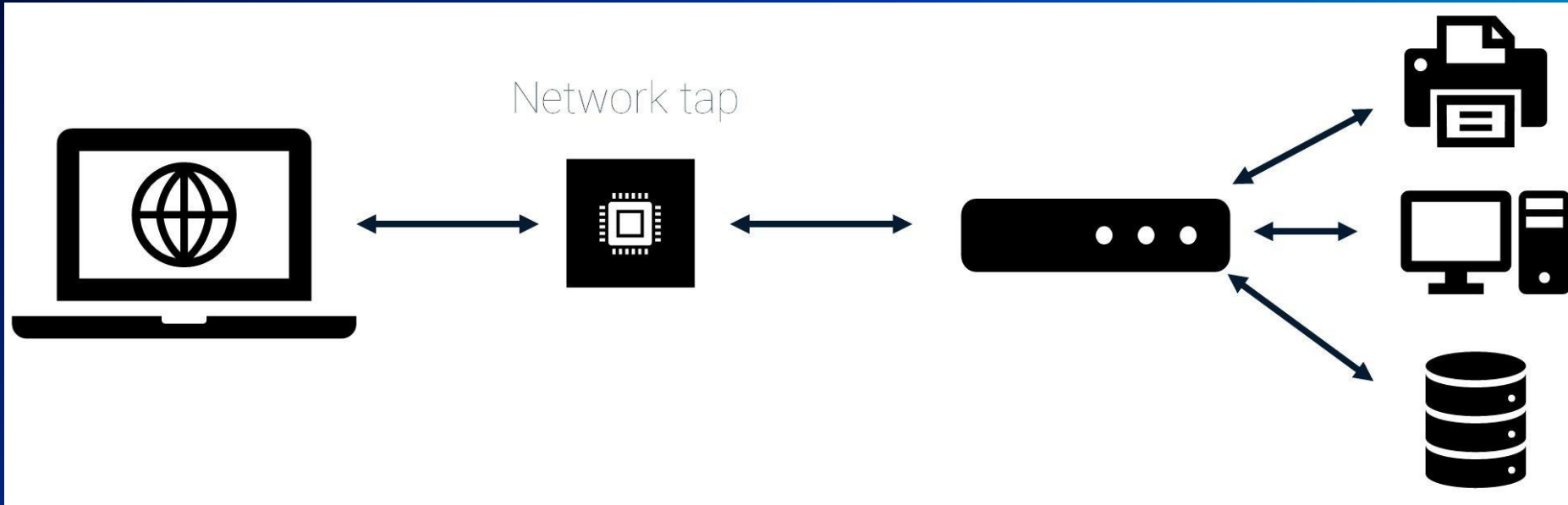


Wireless Sniffing

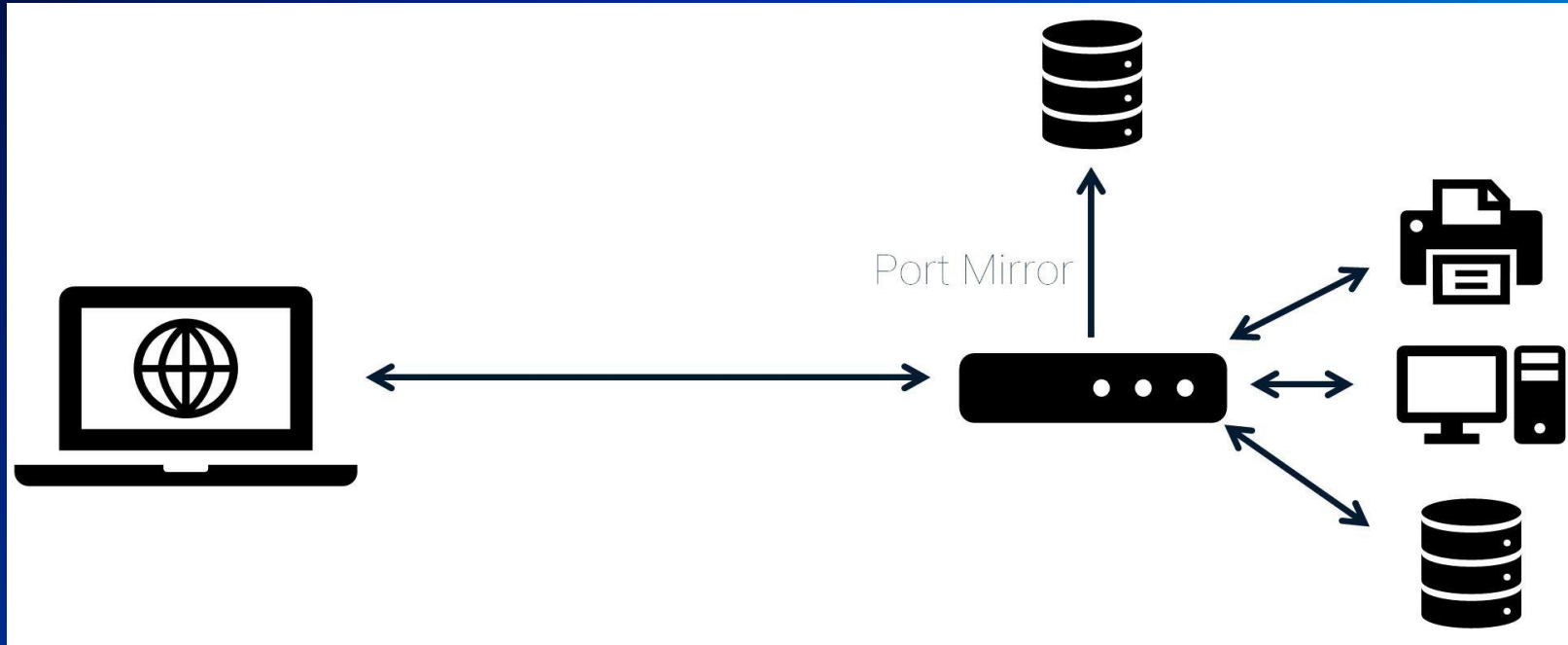
- ◇ Listens over a wireless network for traffic and captures packets



Network Forensics- Capturing Packets



Network Forensics- Capturing Packets



Network Forensics- Capturing Packets



Packets: Examination and Analysis

- ⬡ You can use a packet analyzer, like **Wireshark**, to dive into packets to identify what data was transmitted over a network

Packets

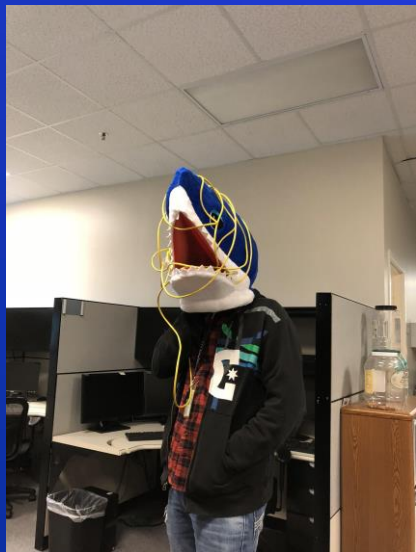
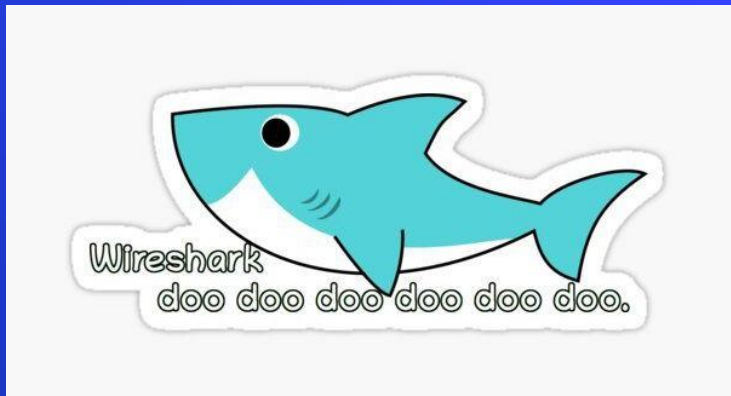
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.101	10.1.1.1	TCP	62	3177 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
2	0.000651	10.1.1.1	10.1.1.101	TCP	62	80 → 3177 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.000697	10.1.1.101	10.1.1.1	TCP	54	3177 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.013669	10.1.1.101	10.1.1.1	HTTP	530	GET / HTTP/1.1
5	0.014730	10.1.1.1	10.1.1.101	TCP	60	80 → 3177 [ACK] Seq=1 Ack=477 Win=6432 Len=0
6	0.032289	10.1.1.1	10.1.1.101	HTTP	489	HTTP/1.1 200 OK (text/html)
7	0.032346	10.1.1.1	10.1.1.101	TCP	60	80 → 3177 [FIN, ACK] Seq=436 Ack=477 Win=6432 Len=0
8	0.032407	10.1.1.101	10.1.1.1	TCP	54	3177 → 80 [ACK] Seq=477 Ack=437 Win=65100 Len=0
9	0.121783	10.1.1.101	209.225.11.237	TCP	62	3179 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
10	0.136302	10.1.1.101	10.1.1.1	TCP	54	3177 → 80 [FIN, ACK] Seq=477 Ack=437 Win=65100 Len=0

Details

▶ Frame 9: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▶ Ethernet II, Src: SmcNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: D-Link_6f:d7:c1 (00:05:5d:6f:d7:c1)
▶ Internet Protocol Version 4, Src: 10.1.1.101, Dst: 209.225.11.237
▶ Transmission Control Protocol, Src Port: 3179, Dst Port: 80, Seq: 0, Len: 0

Hexadecimal

0000	00 05 5d 6f d7 c1 00 04 e2 22 5a 03 08 00 45 00	...jo... "Z...E...
0010	00 30 b3 0a 40 00 08 06 5e 89 0a 01 01 65 d1 e1	-0-@...^...e...
0020	0b ed 0c 6b 00 50 34 9d 5c bc 00 00 00 70 02	...k P4- \...p...
0030	00 00 fb d6 00 00 02 04 05 b4 01 01 04 02

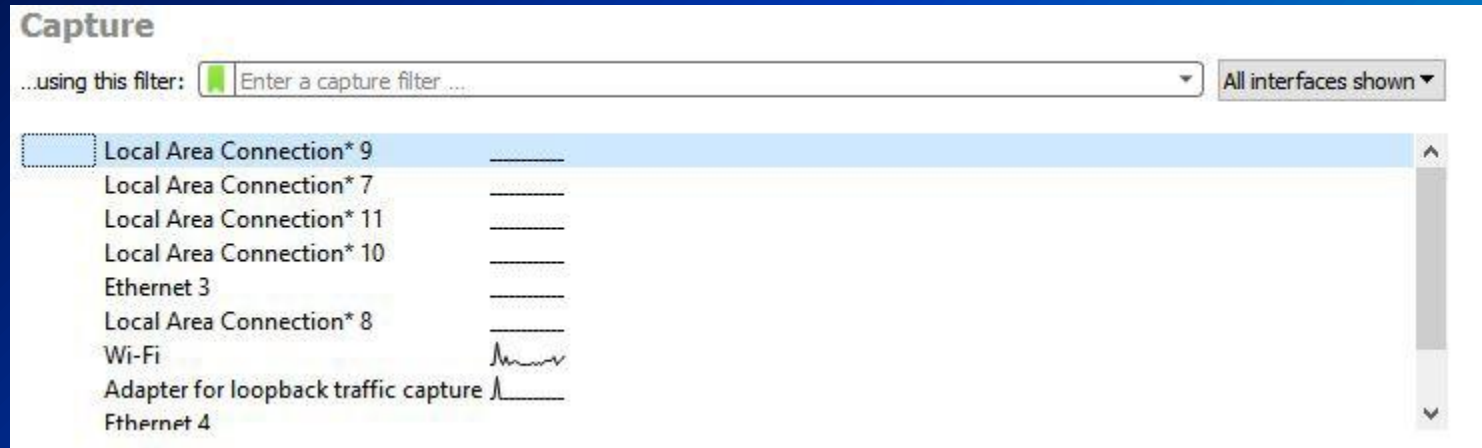


Break Time!



Demo: Introduction to Wireshark

Capturing packets from your network adapter



Stopping your packet capture and examining results...

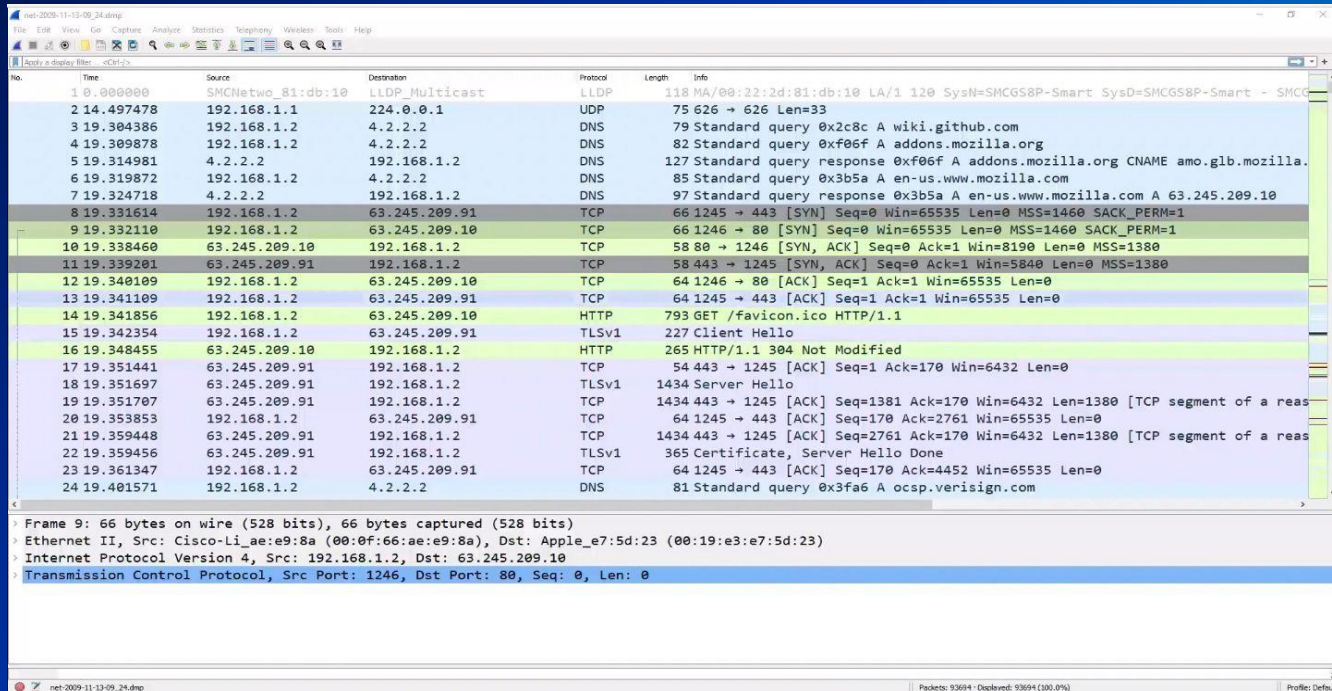
The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows a detailed view of a selected packet, specifically a User Datagram Protocol (UDP) packet and its Domain Name System (DNS) query.

No.	Time	Source	Destination	Protocol	Length	Info
161	19:20:15.575108			DNS	107	Standard query response 0x1c6e AAAA gsas.nyu.edu CNAM
162	19:20:15.575697			DNS	71	Standard query 0x93fa AAAA twitter.com
163	19:20:15.580920			DNS	156	Standard query response 0x7a74 AAAA cas.nyu.edu CNAME
164	19:20:15.581425			DNS	72	Standard query 0xdffe AAAA home.nyu.edu
165	19:20:15.586816			DNS	157	Standard query response 0x1c6e AAAA gsas.nyu.edu CNAM
166	19:20:15.603485			TCP	74	55981 → 80 [ACK] Seq=516 Ack=4990 Win=64252 Len=0
167	19:20:15.608104			DNS	72	Standard query response 0xdffe AAAA home.nyu.edu
168	19:20:15.608802			DNS	73	Standard query 0x2596 AAAA medli.nyu.edu
169	19:20:15.614226			DNS	137	Standard query response 0x7784 A www.instagram.com CN
170	19:20:15.618414			DNS	77	Standard query 0x15a2 AAAA www.instagram.com
171	19:20:15.620176			DNS	73	Standard query response 0x2596 AAAA medli.nyu.edu
172	19:20:15.620767			DNS	75	Standard query 0x0110 AAAA nursing.nyu.edu
173	19:20:15.621333			DNS	143	Standard query response 0x93fa AAAA twitter.com SOA n
174	19:20:15.621761			DNS	67	Standard query 0x6baf A nyu.edu
175	19:20:15.621862			DNS	67	Standard query 0xd581 AAAA nyu.edu
176	19:20:15.635305			DNS	75	Standard query response 0x0110 AAAA nursing.nyu.edu
177	19:20:15.635875			DNS	73	Standard query 0xf669 A nyuad.nyu.edu
178	19:20:15.635977			DNS	73	Standard query 0x65c7 AAAA nyuad.nyu.edu
179	19:20:15.640669			DNS	149	Standard query response 0x15a2 AAAA www.instagram.com
180	19:20:15.641173			DNS	80	Standard query 0x9cac AAAA publichealth.nyu.edu
181	19:20:15.653003			DNS	67	Standard query response 0xd581 AAAA nyu.edu
182	19:20:15.675812			DNS	80	Standard query response 0x9cac AAAA publichealth.nyu.

User Datagram Protocol, Src Port: 55886, Dst Port: 53
Domain Name System (query)

```
0000  b8 27 eb 4e a4 de c8 58  c0 25 ac 4c 08 00 45 00  .N...X .%.L..E.
0010  00 3a 29 18 00 00 80 11  00 00 c0 a8 00 d7 c0 a8  .:)... ..
0020  00 fa da 4e 00 35 00 26  83 59 df fe 01 00 00 01  .N-5& .Y.....
0030  00 00 00 00 00 00 04 68  6f 6d 65 03 6e 79 75 03  .....h ome-nyu-
0040  65 64 75 00 00 1c 00 01  edu.....
```

Overview of the packet list



The image shows a screenshot of the Wireshark network protocol analyzer. The main window displays a list of captured packets, with the first 24 packets visible. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The packets show a mix of DNS queries and responses, TCP SYN and ACK segments, and an HTTP GET request. The details pane at the bottom shows the structure of the selected packet (Frame 9), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SMCNetwo_81:db:10	LLDP_Multicast	LLDP	118	MA/00:22:2d:81:db:10 LA/1 120 SysN=SMCGS8P-Smart SysD=SMCGS8P-Smart - SMC
2	14.497478	192.168.1.1	224.0.0.1	UDP	75	626 → 626 Len=33
3	19.304386	192.168.1.2	4.2.2.2	DNS	79	Standard query 0x2c8c A wiki.github.com
4	19.309878	192.168.1.2	4.2.2.2	DNS	82	Standard query 0xf06f A addons.mozilla.org
5	19.314981	4.2.2.2	192.168.1.2	DNS	127	Standard query response 0xf06f A addons.mozilla.org CNAME amo.glb.mozilla.
6	19.319872	192.168.1.2	4.2.2.2	DNS	85	Standard query 0x3b5a A en-us.www.mozilla.com
7	19.324718	4.2.2.2	192.168.1.2	DNS	97	Standard query response 0x3b5a A en-us.www.mozilla.com A 63.245.209.10
8	19.331614	192.168.1.2	63.245.209.91	TCP	66	1245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
9	19.332110	192.168.1.2	63.245.209.10	TCP	66	1245 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
10	19.338460	63.245.209.10	192.168.1.2	TCP	58	80 → 1245 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
11	19.339201	63.245.209.91	192.168.1.2	TCP	58	443 → 1245 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
12	19.340109	192.168.1.2	63.245.209.10	TCP	64	1245 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
13	19.341109	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
14	19.341856	192.168.1.2	63.245.209.10	HTTP	793	GET /favicon.ico HTTP/1.1
15	19.342354	192.168.1.2	63.245.209.91	TLSv1	227	Client Hello
16	19.348455	63.245.209.10	192.168.1.2	HTTP	265	HTTP/1.1 304 Not Modified
17	19.351441	63.245.209.91	192.168.1.2	TCP	54	443 → 1245 [ACK] Seq=1 Ack=170 Win=6432 Len=0
18	19.351697	63.245.209.91	192.168.1.2	TLSv1	1434	Server Hello
19	19.351707	63.245.209.91	192.168.1.2	TCP	1434	443 → 1245 [ACK] Seq=1381 Ack=170 Win=6432 Len=1380 [TCP segment of a reas
20	19.353853	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=170 Ack=2761 Win=65535 Len=0
21	19.359448	63.245.209.91	192.168.1.2	TCP	1434	443 → 1245 [ACK] Seq=2761 Ack=170 Win=6432 Len=1380 [TCP segment of a reas
22	19.359456	63.245.209.91	192.168.1.2	TLSv1	365	Certificate, Server Hello Done
23	19.361347	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=170 Ack=4452 Win=65535 Len=0
24	19.401571	192.168.1.2	4.2.2.2	DNS	81	Standard query 0x3fa6 A ocsip.verisign.com

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco-Li_ae:e9:8a (00:0f:66:ae:e9:8a), Dst: Apple_e7:5d:23 (00:19:e3:e7:5d:23)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 63.245.209.10
Transmission Control Protocol, Src Port: 1246, Dst Port: 80, Seq: 0, Len: 0

Protocol hierarchy statistics

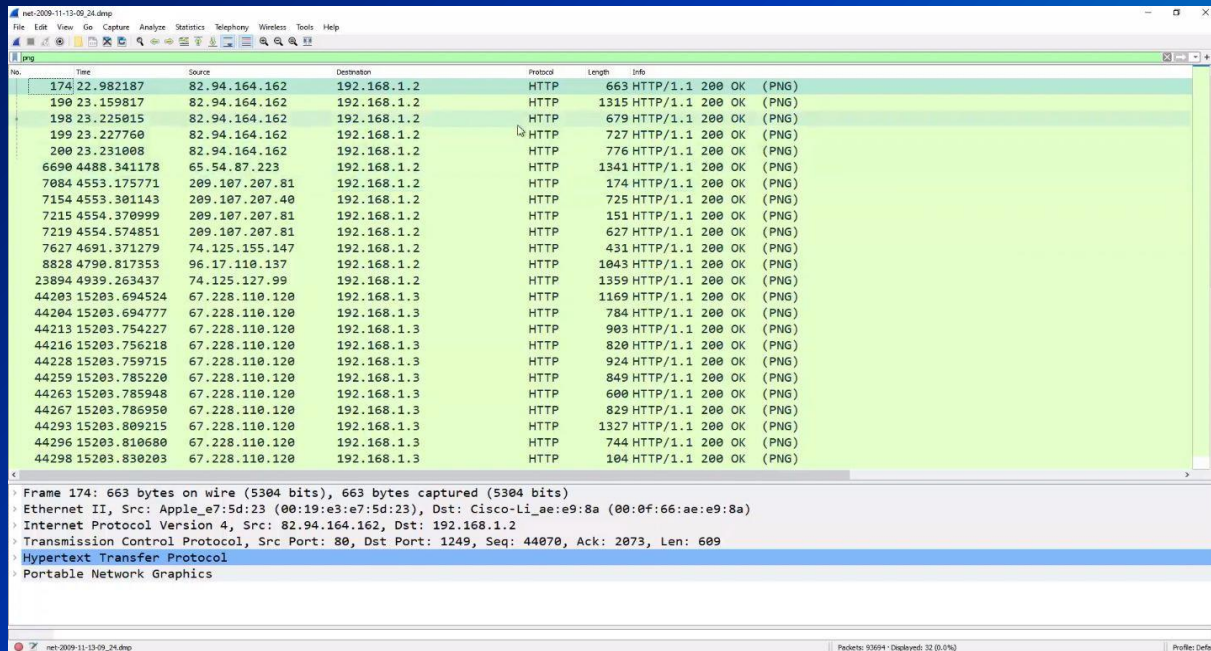
Wireshark - Protocol Hierarchy Statistics - net-2009-11-13-09_24.dmp

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	93694	100.0	62302990	5769	0	0	0
Ethernet	100.0	93694	2.1	1311716	121	0	0	0
Link Layer Discovery Protocol	3.1	2878	0.5	289312	27	2878	289312	27
Internet Protocol Version 6	0.4	373	0.0	14920	1	0	0	0
User Datagram Protocol	0.3	324	0.0	2592	0	0	0	0
Multicast Domain Name System	0.2	226	0.1	50023	4	226	50023	4
Link-local Multicast Name Resolution	0.0	8	0.0	206	0	8	206	0
DHCPv6	0.1	74	0.0	6586	0	74	6586	0
Data	0.0	16	0.0	14554	1	16	14554	1
Internet Control Message Protocol v6	0.1	49	0.0	1196	0	49	1196	0
Internet Protocol Version 4	95.5	88441	2.9	1788900	165	0	0	0
User Datagram Protocol	17.9	16762	0.2	134096	12	0	0	0
Simple Service Discovery Protocol	0.1	78	0.0	10372	0	78	10372	0
Network Time Protocol	2.3	2161	0.2	103728	9	2161	103728	9
NetBIOS Name Service	0.7	688	0.1	38114	3	688	38114	3
NetBIOS Datagram Service	0.4	406	0.1	81320	7	0	0	0
SMB (Server Message Block Protocol)	0.4	406	0.1	48028	4	0	0	0
SMB MailSlot Protocol	0.4	406	0.0	10190	0	0	0	0
Microsoft Windows Browser Protocol	0.4	406	0.0	13112	1	406	13112	1
NAT Port Mapping Protocol	0.0	4	0.0	56	0	4	56	0
Multicast Domain Name System	0.3	249	0.1	53799	4	249	53799	4
Link-local Multicast Name Resolution	0.0	8	0.0	206	0	8	206	0
Dynamic Host Configuration Protocol	0.4	335	0.2	101967	9	335	101967	9
Domain Name System	10.6	9928	1.0	629505	58	9928	629505	58
Data	3.1	2905	0.2	109756	10	2905	109756	10
Transmission Control Protocol	77.5	72655	91.9	57271944	5303	68929	57543076	5329
Transport Layer Security	0.4	369	0.8	499631	46	358	480655	44
NetBIOS Session Service	0.9	836	0.1	68106	6	228	8740	0
SMB (Server Message Block Protocol)	0.6	608	0.1	56934	5	418	33668	3
SMB Pipe Protocol	0.2	190	0.0	3306	0	0	0	0
Microsoft Windows Lanman Remote API Protocol	0.2	190	0.0	8790	0	190	8790	0
Malformed Packet	0.0	15	0.0	0	0	15	0	0
Hypertext Transfer Protocol	2.7	2518	61.2	38109859	3529	1121	579224	53
Portable Network Graphics	0.0	32	0.4	268307	24	32	275727	25
Online Certificate Status Protocol	0.0	4	0.0	2039	0	4	2368	0
Media Type	0.5	475	31.9	19890897	1842	475	20031647	1852
Line-based text data	0.5	457	12.3	7648915	708	457	7296910	675
JPEG File Interchange Format	0.0	17	0.3	203113	18	17	206089	19
HTML Form URL Encoded	0.0	6	0.0	1879	0	6	1879	0
extensible Markup Language	0.3	318	0.6	375794	34	318	385190	35
Data	0.1	50	14.6	9120711	844	50	9135257	846
Compulsive GIF	0.0	37	0.1	52501	4	37	56063	5

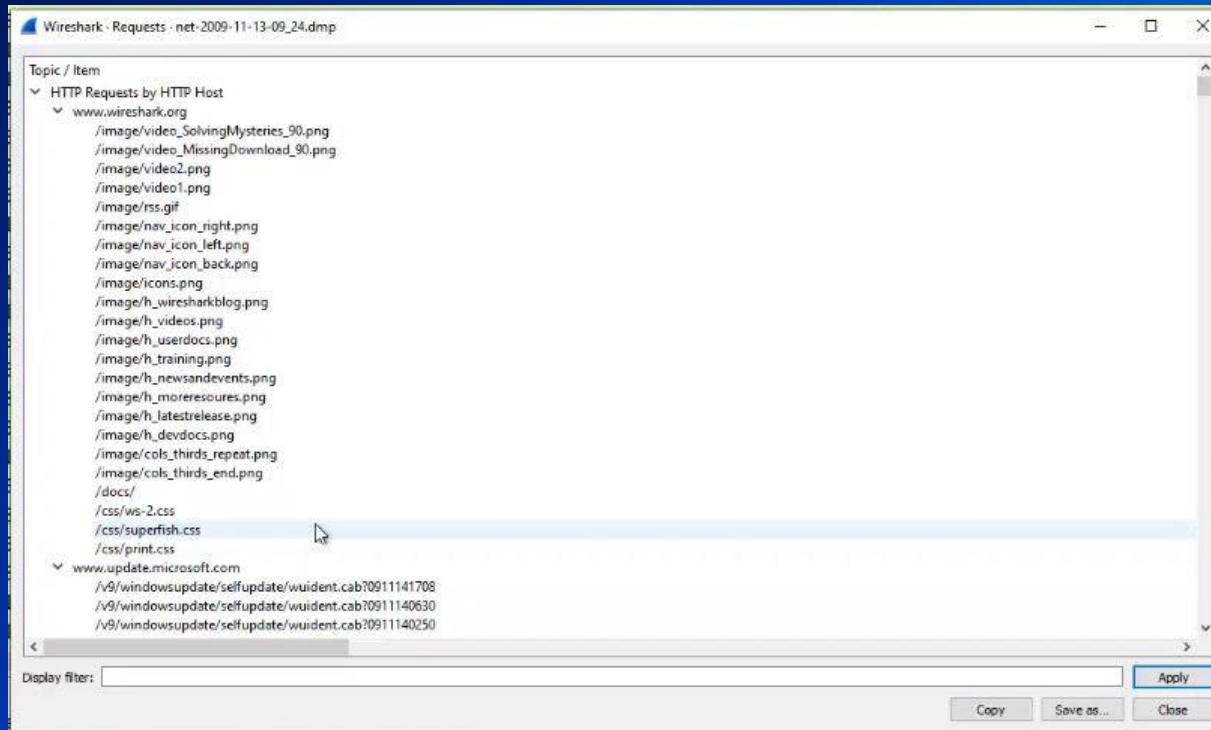
No display filter.

Close Copy Help

Display filters



HTTP request statistics



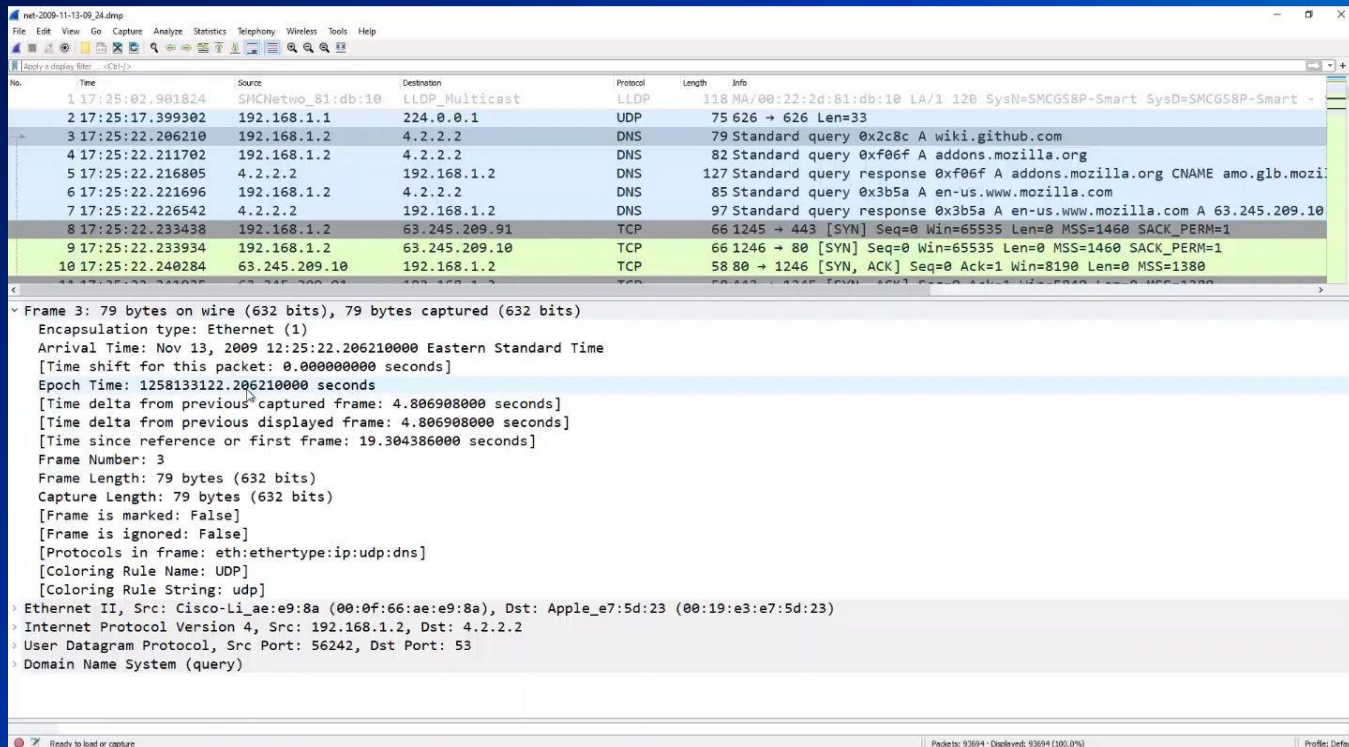
String searches

The image shows a Wireshark packet capture window with a string search filter applied. The filter is '49281-49360'. The packet list shows a series of TCP and HTTP packets. The selected packet is packet 39687, which is an HTTP GET request. The packet details pane shows the following information:

- Frame 39687: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
- Ethernet II, Src: Cisco-Li_ae:e9:8a (00:0f:66:ae:e9:8a), Dst: Apple_e7:5d:23 (00:19:e3:e7:5d:23)
- Internet Protocol Version 4, Src: 192.168.1.2, Dst: 74.125.15.18
- Transmission Control Protocol, Src Port: 1305, Dst Port: 80, Seq: 682, Ack: 4120, Len: 681
- Hypertext Transfer Protocol
 - GET /safebrowsing/rd/goog-phish-shavar_s_49281-49360.49281-49360.: HTTP/1.1\r\n
 - Host: safebrowsing-cache.google.com\r\n
 - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5\r\n

The packet bytes pane shows the raw data of the packet, which is a hexadecimal representation of the HTTP request.

Time settings



Packet details

The image shows a Wireshark packet capture window titled 'net-2008-11-13-08_24.pcap'. The packet list on the left shows a series of DNS queries and responses. The selected packet is a DNS query (No. 3) from 192.168.1.2 to 192.168.1.2, asking for 'wiki.github.com'. The packet details pane on the right shows the structure of this query: User Datagram Protocol (port 56242 to 53), Domain Name System (query), Transaction ID: 0x2c8c, Flags: 0x0100 (Standard query), Questions: 1, Answer RRs: 0, Authority RRs: 0, Additional RRs: 0, and a single query for 'wiki.github.com: type A, class IN'. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII, with the ASCII column displaying 'wiki-github.com'.

No.	Time	Source	Destination	Protocol	Length	Info
1	17:25:02.901824	SMCNetwo_81:db:10	LLDP_Multicast	LLDP	118	MA/00:22:2d:81:db:10 LA/1 120 SysN=SMCGS8P-Smart SysD=SMCGS8P-Smart
2	17:25:17.399302	192.168.1.1	224.0.0.1	UDP	75	626 → 626 Len=33
3	17:25:22.206210	192.168.1.2	4.2.2.2	DNS	79	Standard query 0x2c8c A wiki.github.com
4	17:25:22.211702	192.168.1.2	4.2.2.2	DNS	82	Standard query 0xf06f A addons.mozilla.org
5	17:25:22.216805	4.2.2.2	192.168.1.2	DNS	127	Standard query response 0xf06f A addons.mozilla.org CNAME amo.glb.mozil
6	17:25:22.221696	192.168.1.2	4.2.2.2	DNS	85	Standard query 0x3b5a A en-us.www.mozilla.com
7	17:25:22.226542	4.2.2.2	192.168.1.2	DNS	97	Standard query response 0x3b5a A en-us.www.mozilla.com A 63.245.209.10
8	17:25:22.233438	192.168.1.2	63.245.209.91	TCP	66	1245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
9	17:25:22.233934	192.168.1.2	63.245.209.10	TCP	66	1246 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
10	17:25:22.240284	63.245.209.10	192.168.1.2	TCP	58	80 → 1246 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380

User Datagram Protocol, Src Port: 56242, Dst Port: 53

Domain Name System (query)

- Transaction ID: 0x2c8c
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - wiki.github.com: type A, class IN
- [Response In: 27]

0000 00 19 e3 e7 5d 23 00 0f 66 ae e9 8a 08 00 45 00 ...]#... f...E

0010 00 3d 0a 5a 00 00 80 11 68 a8 c0 a8 01 02 04 02 ...=Z...h.....

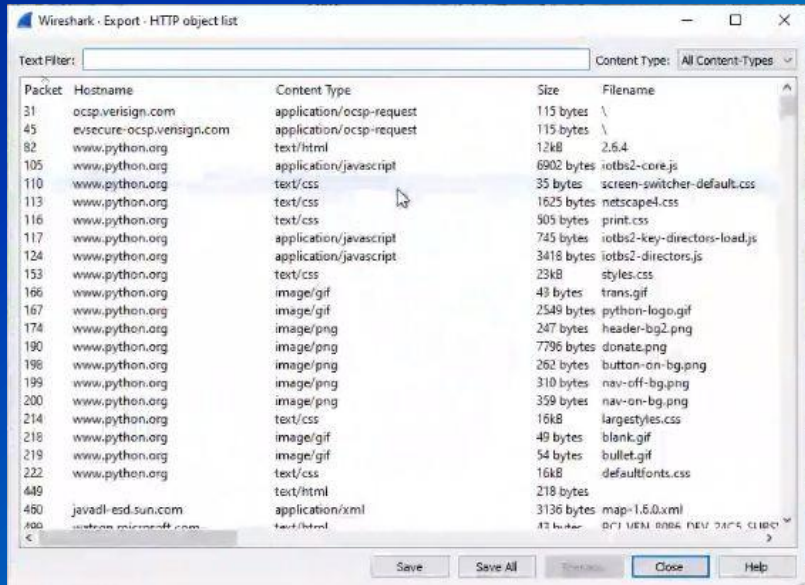
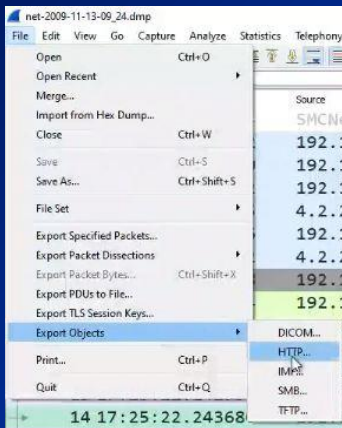
0020 02 02 db b2 00 35 00 29 91 8b 2c 8c 01 00 00 01 ...5)... ..

0030 00 00 00 00 00 04 77 69 6b 69 06 67 69 74 68wiki-gith

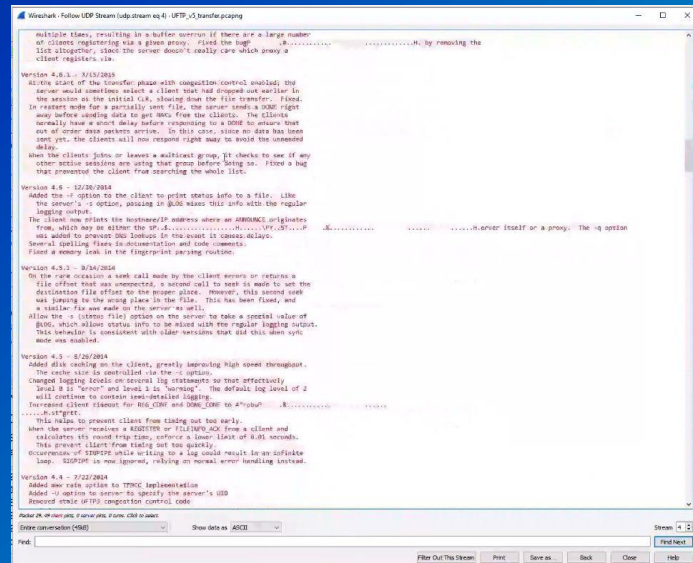
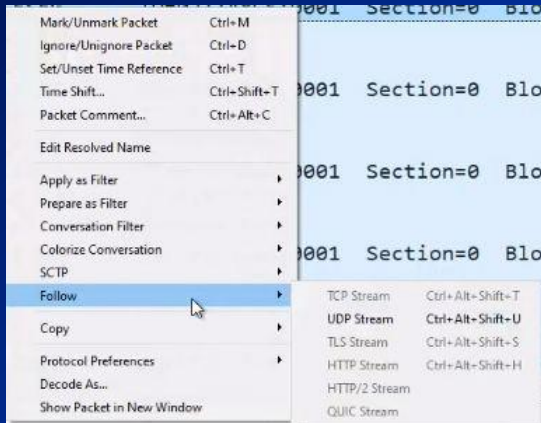
0040 75 62 03 63 6f 6d 00 00 01 00 01 c1 7f 0b f7ub.com.....



Export objects



Following packet streams



Guided Exercise: Capturing and Analyzing Packets

Steps:

- ❖ Open Wireshark
- ❖ Find the active network interface and double-click to start the capture
- ❖ Open a web browser and navigate to <http://www.buffalony.gov/>
- ❖ Close your browser and stop the packet capture
- ❖ Open the protocol hierarchy statistics window and note the protocols
- ❖ Filter the packet list to display HTTP traffic
- ❖ Run a string search for buffalony.gov
- ❖ Export HTTP objects and note the files that were transferred (hint: you may have to manually change the filename to a valid image file)

Summary

- ⬡ Packets are powerful, but require infrastructure considerations to capture, store, and analyze
- ⬡ Encrypted traffic can hinder the effectiveness of packet analysis activities
- ⬡ Tools, like Wireshark, are instrumental in analyzing network traffic and identifying patterns of activity and data transmitted across a network

Homework

⬡ You have been provided with a PCAP (packet capture) file. Your job is to review the network traffic to identify the “flags” hidden throughout. There are 5 flags. For each flag you capture, provide the following information:

- ⬡ The flag itself
- ⬡ A brief description of the type of network traffic examined to identify the flag (e.g., protocol, source, destination) (1-2 sentences)
- ⬡ A screenshot of the captured flag (from Wireshark, or exported files from Wireshark)

⬡ Hints!

- ⬡ Remember the exercises today-- use the Wireshark functions you learned to find the flags!

Homework

- ⬡ Flag 1: Haveibeenpwned?
 - ⬢ What is the email address of the user involved in this network activity?
- ⬡ Flag 2: What's the password?
 - ⬢ The user logs into a server (or servers) with a specific password, what is it?
- ⬡ Flag 3: Switching things up...
 - ⬢ The user tries to change the above password, but can't. Why not?
- ⬡ Flag 4: Hidden in plain sight...
 - ⬢ The user has accessed three files over FTP, but one in particular looks suspicious. What is the file?
- ⬡ Flag 5: Higher-level thinking...
 - ⬢ What are all of the protocols used throughout this PCAP? Of the identified protocols, document the security significance of at least one of them.

Additional Resources

- Autopsy (Digital Forensics Platform and Graphical Interface)
<https://www.autopsy.com/>
- Wireshark Wiki - Sample Captures
<https://wiki.wireshark.org/SampleCaptures>
- Wireshark User's Guide (Advanced Topics = Chapter 7)
https://www.wireshark.org/docs/wsug_html/
- FTK Imager (Data Preview and Imaging Tool)
[https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager#:~:text=FTK%C2%AE%20Imager%20is%20a,%C2%AE%20\(FTK\)%20is%20warranted.](https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager#:~:text=FTK%C2%AE%20Imager%20is%20a,%C2%AE%20(FTK)%20is%20warranted.)

**If you have any questions,
please DM us on mattermost
or come to Office Hours!**