Digital Forensics & Packet Analysis

UBNetDef, Spring 2021

Week 13

Lead Presenter: Dominic Sellitto

Special Thanks: Nick Richter

About Me

- Education
  - Bachelor of Science, Business Administration
  - Master of Science, MIS
- Security Experience
  - Consultant/Senior Consultant, Cyber Risk services, Deloitte
  - Lead Cybersecurity Consultant, Loptr LLC
- Professional Affiliations
  - ISC^2; Certified Information Systems Security Professional (CISSP)
  - Buffalo Electronic Crimes Task Force
- Publications:
  - Vulnerability Assessment (ISACA, 2017)
- Hats worn:
  - Virtual CISO
  - Project Manager
  - Security Analyst
  - Security Monitoring Analyst
  - Security Architect
  - Software Developer

Dominic Sellitto, CISSP

vCISO

Skills

Agenda

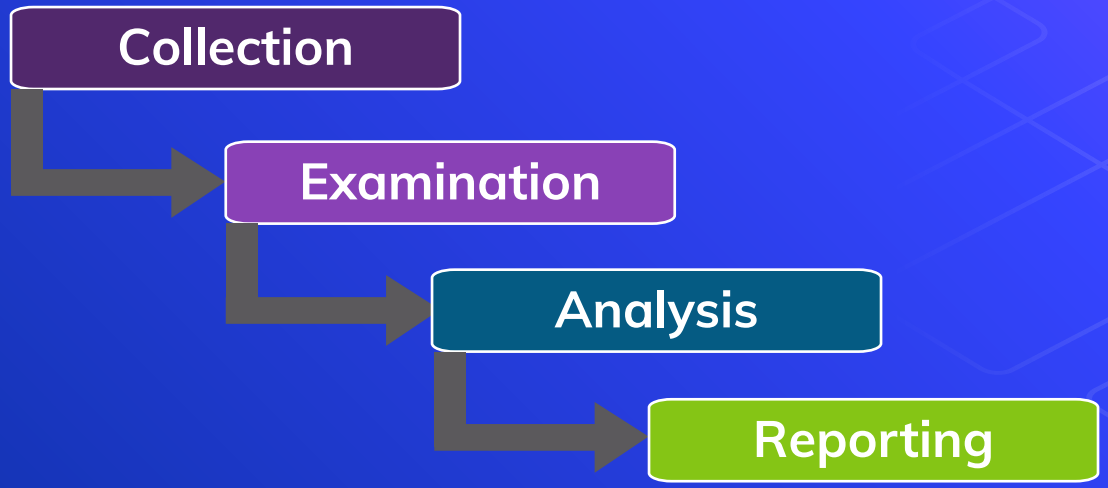
1. Digital Forensics Overview
2. Subdomains within Digital Forensics
3. Network Forensics Overview
4. Wireshark Exercise 1
5. Wireshark Exercise 2
6. Homework

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:



Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

Enabling Factors

- In order to repeatedly execute the process, you need some things…

Governance:
- Policies
- Procedures
- Standards

Finances:
- Tools
- Technologies
- Training

Collection → Examination → Analysis → Reporting

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

Location:
- Lab/Room
- Access Control
- Monitoring

Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

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

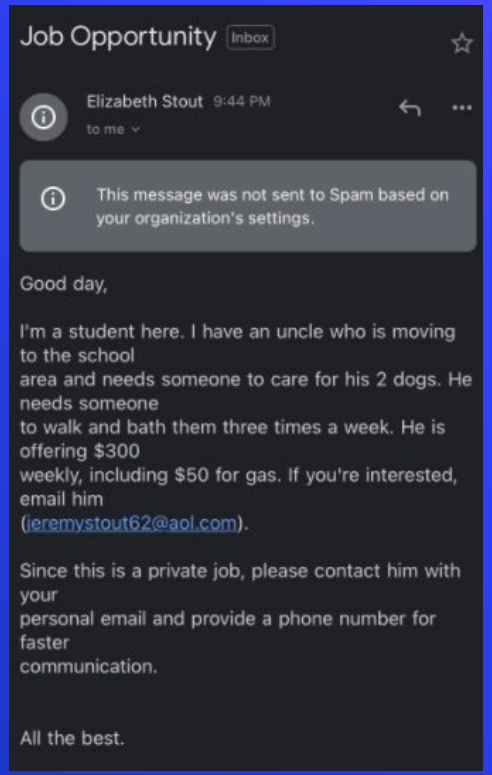
Digital Media Manipulation

- Which of these is fake?

Malware Analysis...

- What's that program ***really*** doing?

Email Forensics...



Job Opportunity Inbox

Elizabeth Stout 9:44 PM
to me

This message was not sent to Spam based on your organization's settings.

Good day,

I'm a student here. I have an uncle who is moving to the school
area and needs someone to care for his 2 dogs. He needs someone
to walk and bath them three times a week. He is offering $300
weekly, including $50 for gas. If you're interested, email him
(jeremystout62@aol.com).

Since this is a private job, please contact him with your
personal email and provide a phone number for faster
communication.

All the best.

Network Forensics

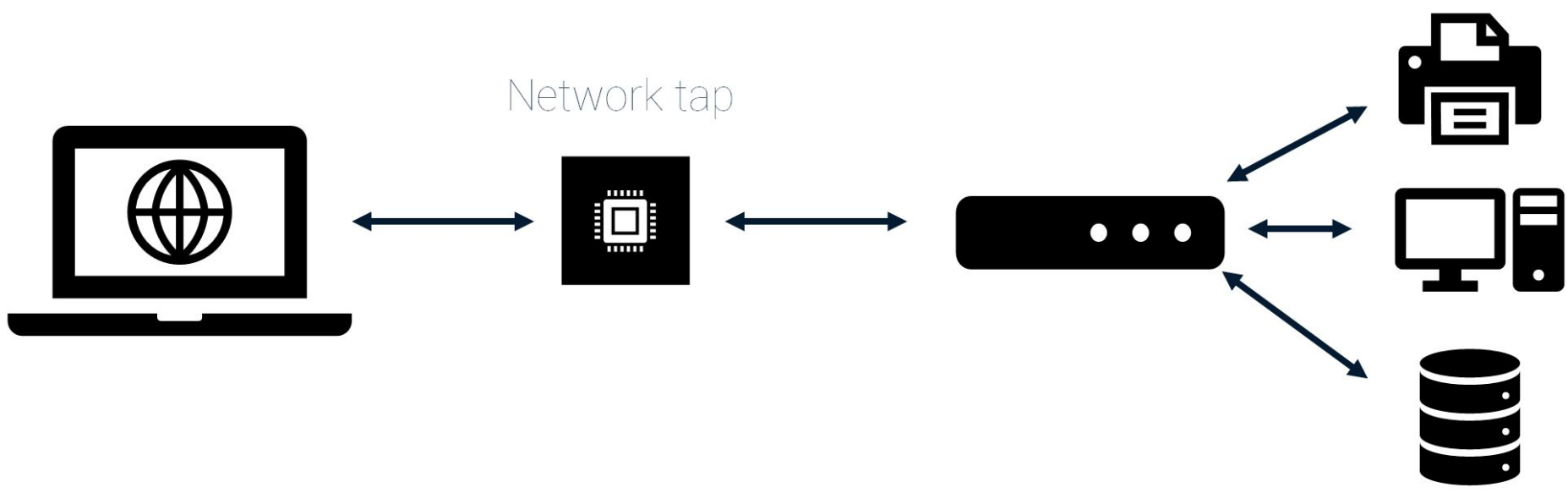
- **Packets** contain all of the information being sent across a network, including the source and destination machine, protocol being used, and the actual data being sent
- **Network logs** are records of network events - they tell you that something happened over the network (like source, destination,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

Network Forensics- Capturing Packets

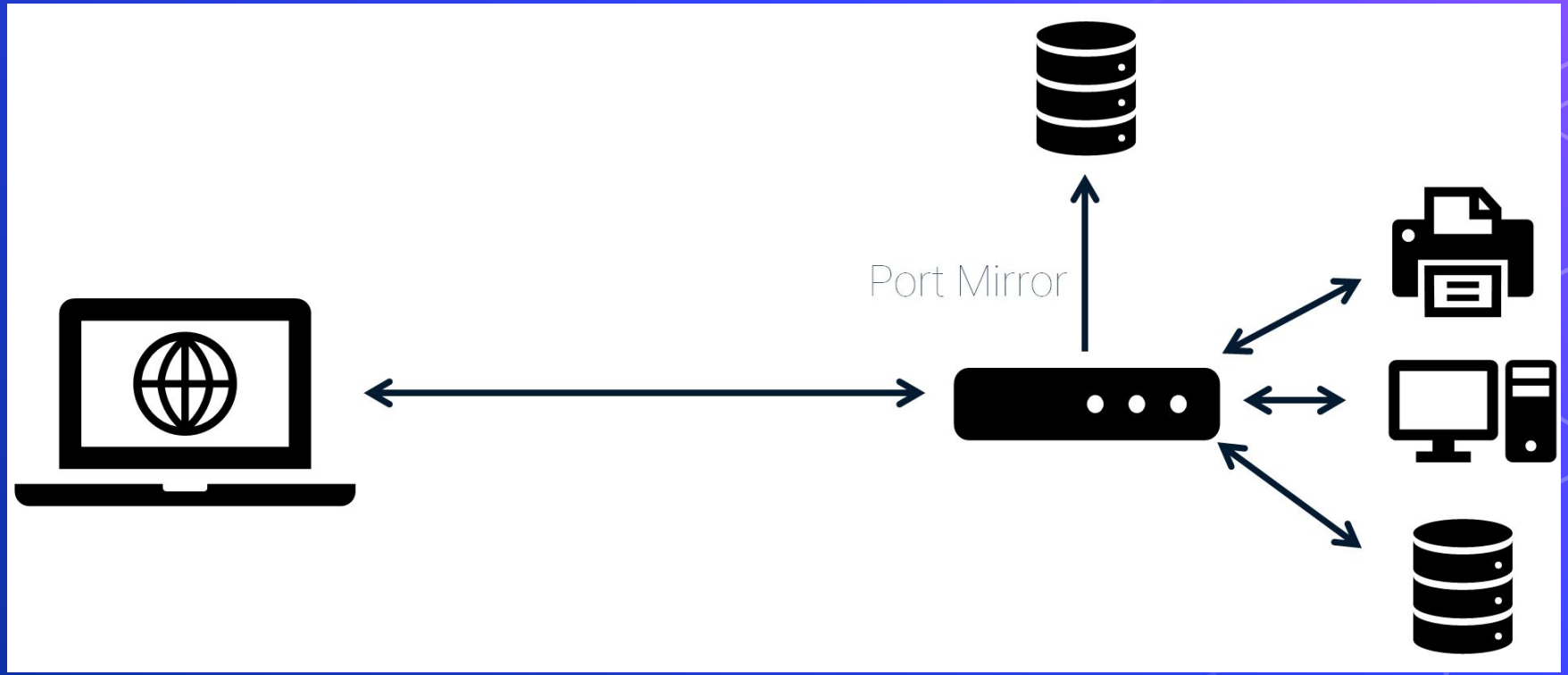
Packets can be captured using a variety of methods:

- 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

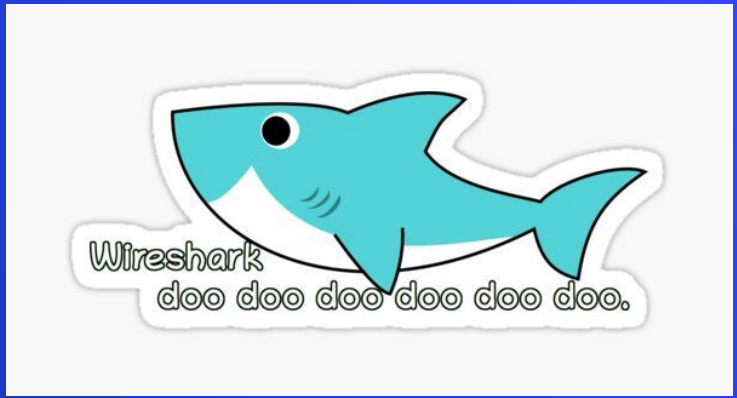
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.1.101	10.1.1.1	TCP	62	3177 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1
2	0.000651	10.1.1.1	10.1.1.101	TCP	62	80 → 3177 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
3	0.000697	10.1.1.101	10.1.1.1	TCP	54	3177 → 80 [ACK] 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

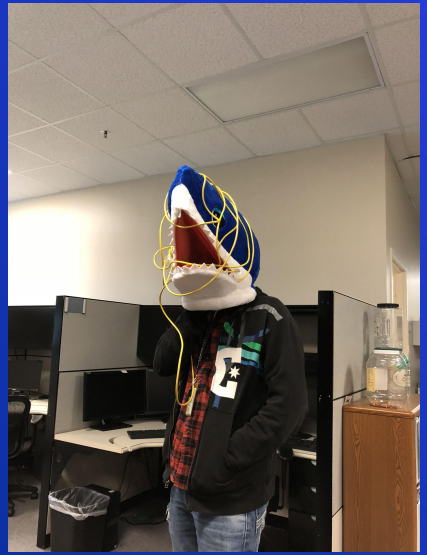
```
▶ Frame 9: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▶ Ethernet II, Src: SmcNetwo_22:5a:03 (00:04:e2:22:5a:03), Dst: D-Link_6f:d7:c1 (00:05:5d:6f:d7:c1)
▶ Internet Protocol Version 4, Src: 10.1.1.101, Dst: 209.225.11.237
▶ Transmission Control Protocol, Src Port: 3179, Dst Port: 80,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

Hexadecimal

```
0000  00 05 5d 6f d7 c1 00 04  e2 22 5a 03 08 00 45 00   ··]o···· ·"Z···E·
0010  00 30 b3 0a 40 00 80 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 00 70 02   ···k·P4· \·····p·
0030  00 00 fb d6 00 00 02 04  05 b4 01 01 04 02         ····· ····· ·····
```


Wireshark
doo doo doo doo doo doo.


PCAP
OR IT
DIDN'T
Happen

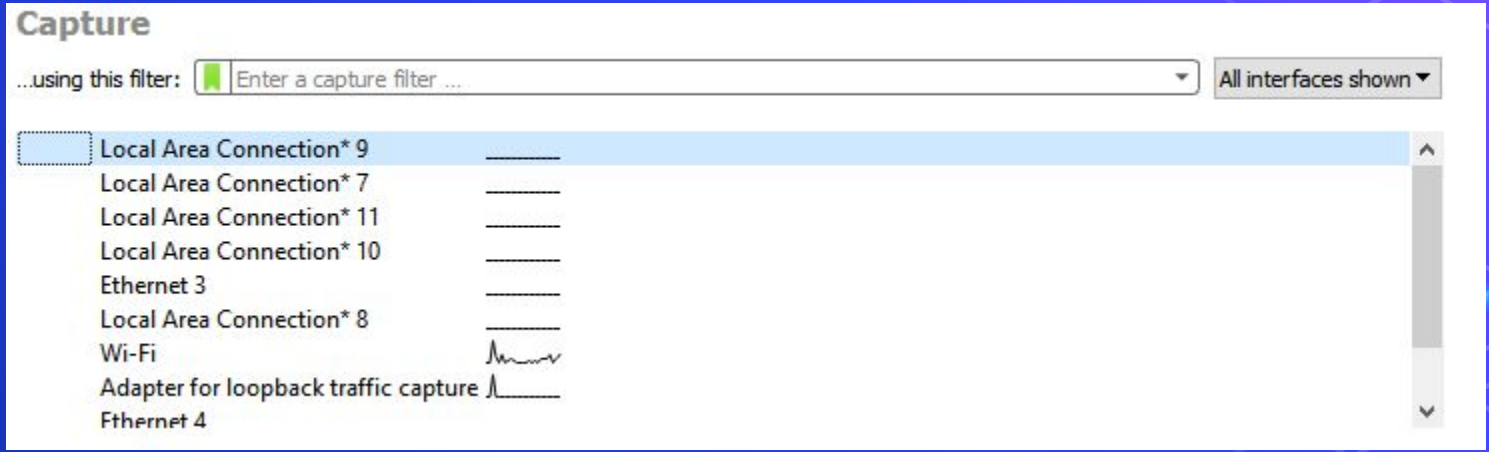


Break Time!

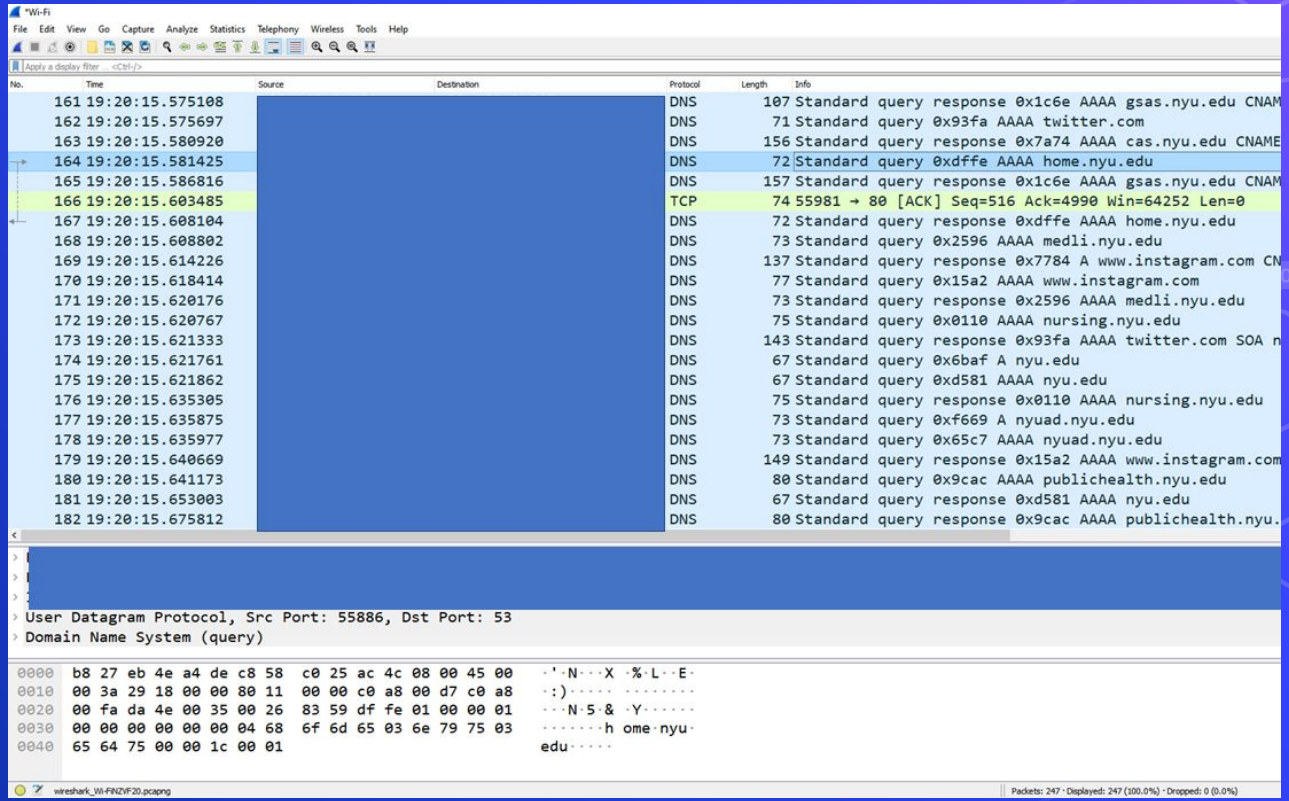

WIRESHARK

Demo: Introduction to Wireshark

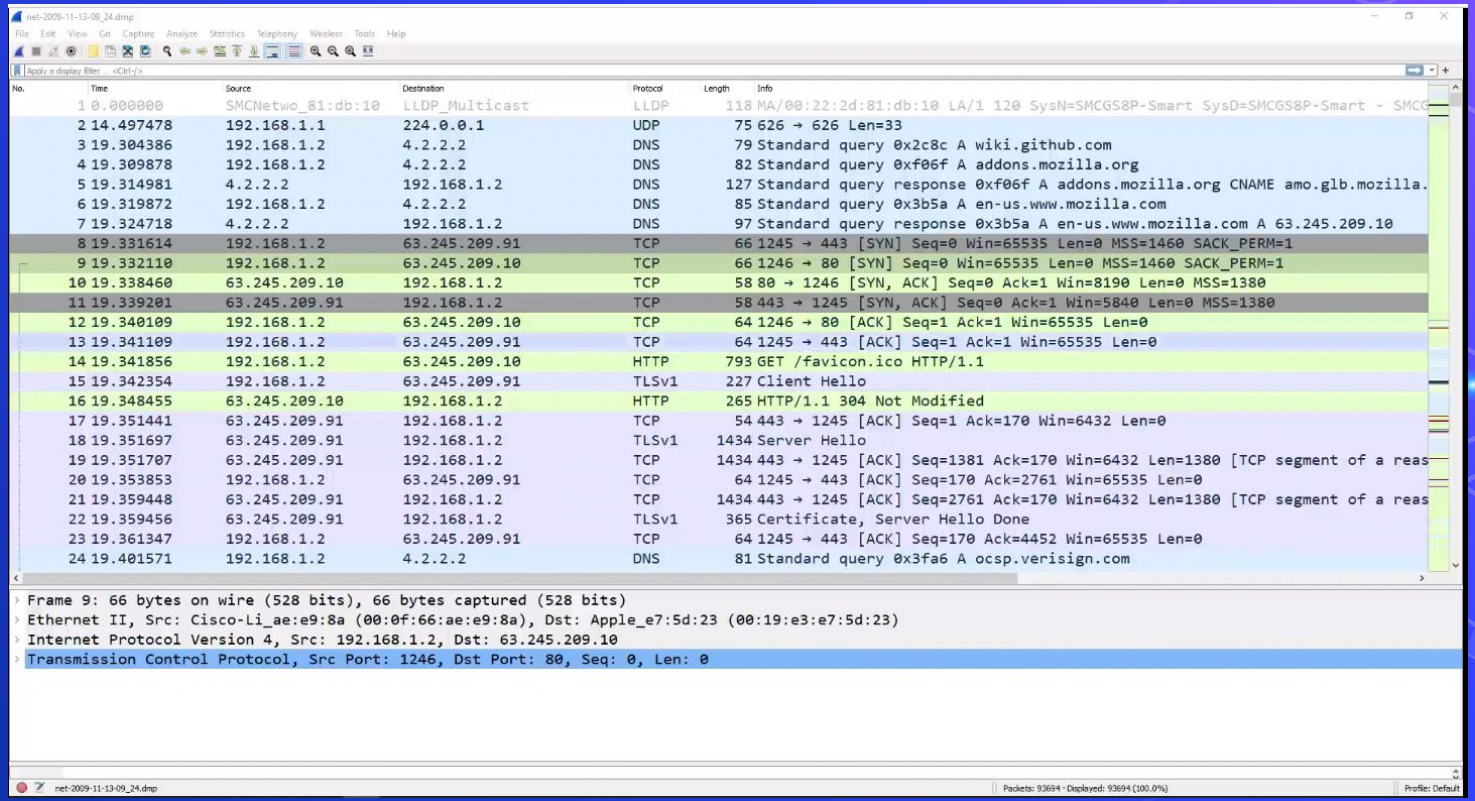
Capturing packets from your network adapter



Stopping your packet capture and examining results...



Overview of the packet list



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	299312	27	2878	299312	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	89441	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	10150	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	8750	0	190	8750	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	20001647	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	209089	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
Compuserve GIF	0.0	37	0.1	52501	4	37	56063	5

No display filter.

Close | Copy | Help

Display filters

net-2009-11-13-09_24.dmp

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

png

No.	Time	Source	Destination	Protocol	Length	Info
174	22.982187	82.94.164.162	192.168.1.2	HTTP	663	HTTP/1.1 200 OK (PNG)
190	23.159817	82.94.164.162	192.168.1.2	HTTP	1315	HTTP/1.1 200 OK (PNG)
198	23.225015	82.94.164.162	192.168.1.2	HTTP	679	HTTP/1.1 200 OK (PNG)
199	23.227760	82.94.164.162	192.168.1.2	HTTP	727	HTTP/1.1 200 OK (PNG)
200	23.231008	82.94.164.162	192.168.1.2	HTTP	776	HTTP/1.1 200 OK (PNG)
6690	4488.341178	65.54.87.223	192.168.1.2	HTTP	1341	HTTP/1.1 200 OK (PNG)
7084	4553.175771	209.107.207.81	192.168.1.2	HTTP	174	HTTP/1.1 200 OK (PNG)
7154	4553.301143	209.107.207.40	192.168.1.2	HTTP	725	HTTP/1.1 200 OK (PNG)
7215	4554.370999	209.107.207.81	192.168.1.2	HTTP	151	HTTP/1.1 200 OK (PNG)
7219	4554.574851	209.107.207.81	192.168.1.2	HTTP	627	HTTP/1.1 200 OK (PNG)
7627	4691.371279	74.125.155.147	192.168.1.2	HTTP	431	HTTP/1.1 200 OK (PNG)
8828	4790.817353	96.17.110.137	192.168.1.2	HTTP	1043	HTTP/1.1 200 OK (PNG)
23894	4939.263437	74.125.127.99	192.168.1.2	HTTP	1359	HTTP/1.1 200 OK (PNG)
44203	15203.694524	67.228.110.120	192.168.1.3	HTTP	1169	HTTP/1.1 200 OK (PNG)
44204	15203.694777	67.228.110.120	192.168.1.3	HTTP	784	HTTP/1.1 200 OK (PNG)
44213	15203.754227	67.228.110.120	192.168.1.3	HTTP	903	HTTP/1.1 200 OK (PNG)
44216	15203.756218	67.228.110.120	192.168.1.3	HTTP	820	HTTP/1.1 200 OK (PNG)
44228	15203.759715	67.228.110.120	192.168.1.3	HTTP	924	HTTP/1.1 200 OK (PNG)
44259	15203.785220	67.228.110.120	192.168.1.3	HTTP	849	HTTP/1.1 200 OK (PNG)
44263	15203.785948	67.228.110.120	192.168.1.3	HTTP	600	HTTP/1.1 200 OK (PNG)
44267	15203.786950	67.228.110.120	192.168.1.3	HTTP	829	HTTP/1.1 200 OK (PNG)
44293	15203.809215	67.228.110.120	192.168.1.3	HTTP	1327	HTTP/1.1 200 OK (PNG)
44296	15203.810680	67.228.110.120	192.168.1.3	HTTP	744	HTTP/1.1 200 OK (PNG)
44298	15203.830203	67.228.110.120	192.168.1.3	HTTP	104	HTTP/1.1 200 OK (PNG)

```
> Frame 174: 663 bytes on wire (5304 bits), 663 bytes captured (5304 bits)
> Ethernet II, Src: Apple_e7:5d:23 (00:19:e3:e7:5d:23), Dst: Cisco-Li_ae:e9:8a (00:0f:66:ae:e9:8a)
> Internet Protocol Version 4, Src: 82.94.164.162, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 1249, Seq: 44070, Ack: 2073, Len: 609
> Hypertext Transfer Protocol
> Portable Network Graphics
```

net-2009-11-13-09_24.dmp Packets: 93694 · Displayed: 32 (0.0%) Profile: Default

HTTP request statistics

Wireshark · Requests · net-2009-11-13-09_24.dmp

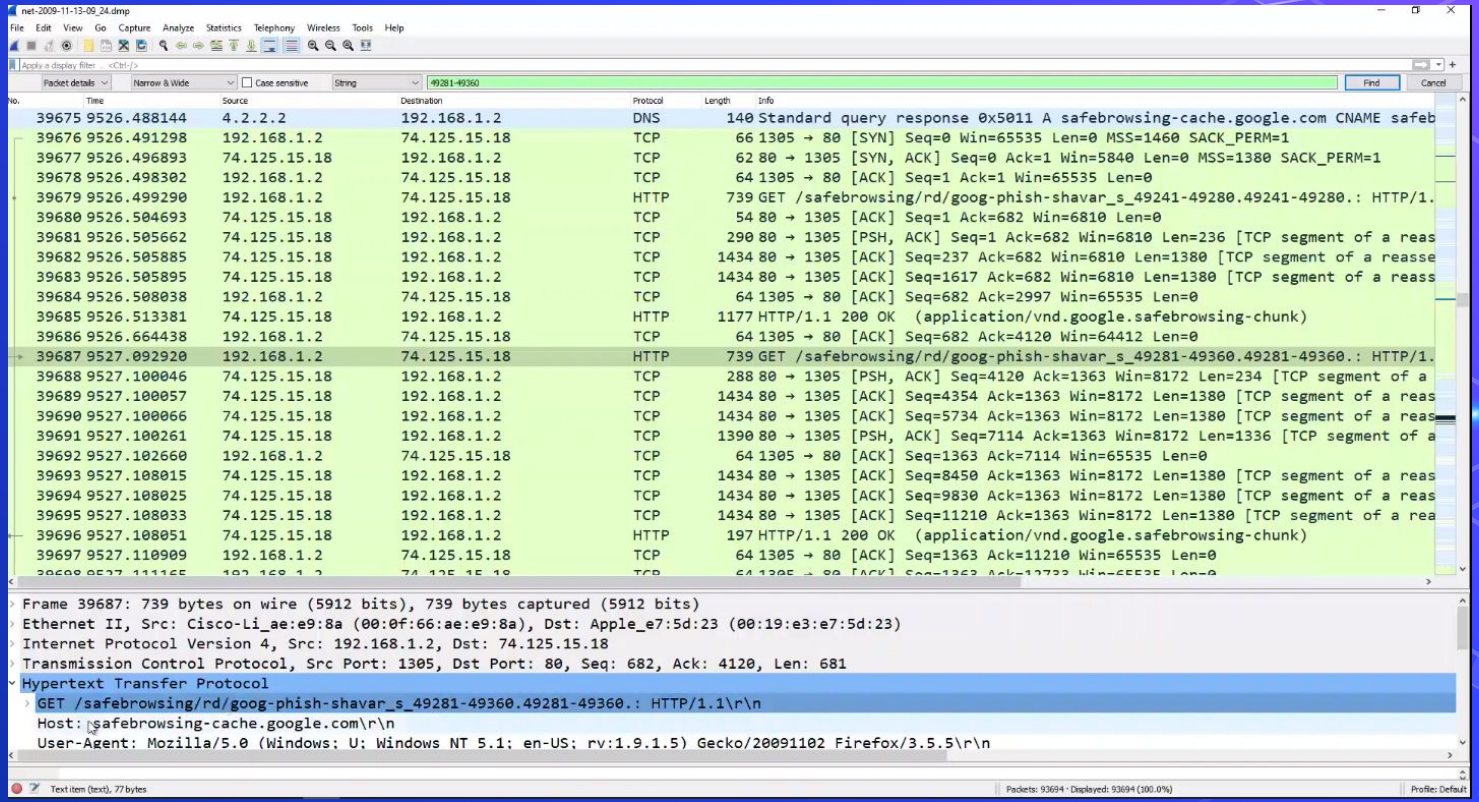
Topic / Item

- HTTP Requests by HTTP Host
  - www.wireshark.org
    - /image/video_SolvingMysteries_90.png
    - /image/video_MissingDownload_90.png
    - /image/video2.png
    - /image/video1.png
    - /image/rss.gif
    - /image/nav_icon_right.png
    - /image/nav_icon_left.png
    - /image/nav_icon_back.png
    - /image/icons.png
    - /image/h_wiresharkblog.png
    - /image/h_videos.png
    - /image/h_userdocs.png
    - /image/h_training.png
    - /image/h_newsandevents.png
    - /image/h_moreresoures.png
    - /image/h_latestrelease.png
    - /image/h_devdocs.png
    - /image/cols_thirds_repeat.png
    - /image/cols_thirds_end.png
    - /docs/
    - /css/ws-2.css
    - /css/superfish.css
    - /css/print.css
  - www.update.microsoft.com
    - /v9/windowsupdate/selfupdate/wuident.cab?0911141708
    - /v9/windowsupdate/selfupdate/wuident.cab?0911140630
    - /v9/windowsupdate/selfupdate/wuident.cab?0911140250

Display filter: Apply

Copy Save as... Close

String searches



Time settings

net-2009-11-13-09_24.dmp

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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

```
Frame 3: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 13, 2009 12:25:22.206210000 Eastern Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1258133122.206210000 seconds
  [Time delta from previous captured frame: 4.806908000 seconds]
  [Time delta from previous displayed frame: 4.806908000 seconds]
  [Time since reference or first frame: 19.304386000 seconds]
  Frame Number: 3
  Frame Length: 79 bytes (632 bits)
  Capture Length: 79 bytes (632 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
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: 4.2.2.2
User Datagram Protocol, Src Port: 56242, Dst Port: 53
Domain Name System (query)
```

Ready to load or capture | Packets: 93694 · Displayed: 93694 (100.0%) | Profile: Default

Packet details

net-2009-11-13-09_24.dmp

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

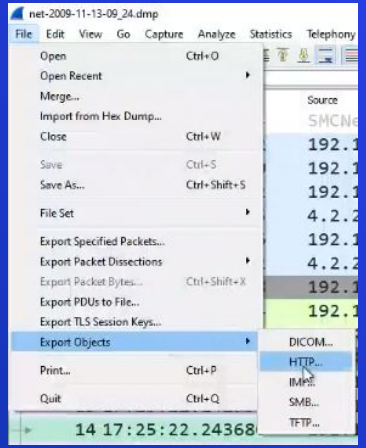
No.	Time	Source	Destination	Protocol	Length	Info
1	17:25:02.901824	SMCNetwo_81:db:10	LLDP_Multicast	LLDP	118	MA/00:22:2d:81:db:10 LA/1 120 SysN=SMCGS8P-Smart SysD=SMCGS8P-Smart -
2	17:25:17.399302	192.168.1.1	224.0.0.1	UDP	75	626 → 626 Len=33
3	17:25:22.206210	192.168.1.2	4.2.2.2	DNS	79	Standard query 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.mozi
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

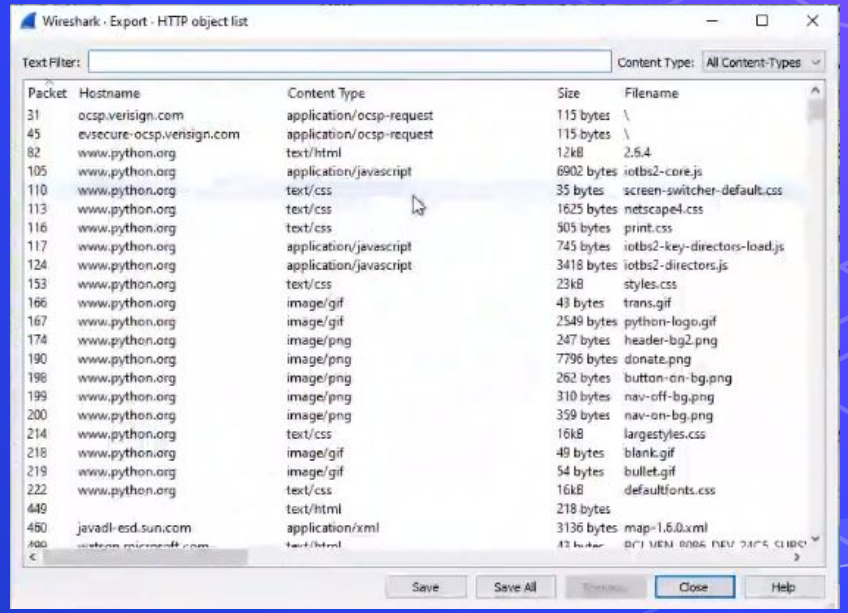
```
> User Datagram Protocol, Src Port: 56242, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x2c8c
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > wiki.github.com: type A, class IN
    [Response In: 27]
```

```
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 00 04 77  69 6b 69 06 67 69 74 68   ·******w iki·gith
0040  75 62 03 63 6f 6d 00 00  01 00 01 c1 7f 0b f7      ub·com·· ·******
```

Text item (text), 21 bytes | Packets: 93694 · Displayed: 93694 (100.0%) | Profile: Default

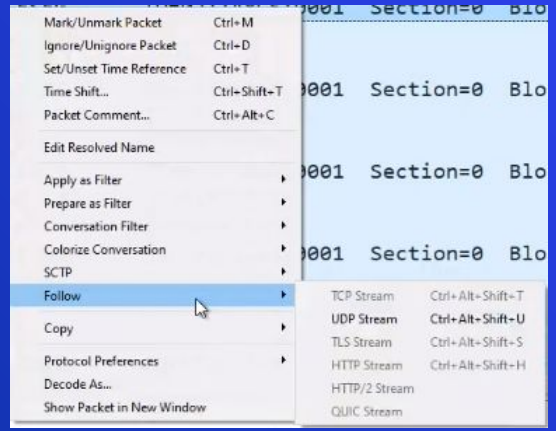
Export objects

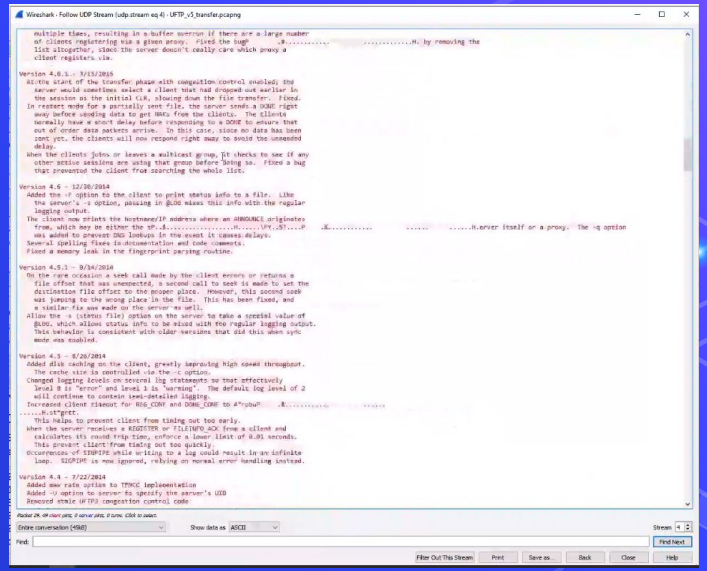




Packet	Hostname	Content Type	Size	Filename
31	ocsp.verisign.com	application/ocsp-request	115 bytes	\
45	evsecure-ocsp.verisign.com	application/ocsp-request	115 bytes	\
82	www.python.org	text/html	12kB	2.6.4
105	www.python.org	application/javascript	6902 bytes	iotbs2-core.js
110	www.python.org	text/css	35 bytes	screen-switcher-default.css
113	www.python.org	text/css	1625 bytes	netscape4.css
116	www.python.org	text/css	505 bytes	print.css
117	www.python.org	application/javascript	745 bytes	iotbs2-key-directors-load.js
124	www.python.org	application/javascript	3418 bytes	iotbs2-directors.js
153	www.python.org	text/css	23kB	styles.css
166	www.python.org	image/gif	43 bytes	trans.gif
167	www.python.org	image/gif	2549 bytes	python-logo.gif
174	www.python.org	image/png	247 bytes	header-bg2.png
190	www.python.org	image/png	7796 bytes	donate.png
198	www.python.org	image/png	262 bytes	button-on-bg.png
199	www.python.org	image/png	310 bytes	nav-off-bg.png
200	www.python.org	image/png	359 bytes	nav-on-bg.png
214	www.python.org	text/css	16kB	largestyles.css
218	www.python.org	image/gif	49 bytes	blank.gif
219	www.python.org	image/gif	54 bytes	bullet.gif
222	www.python.org	text/css	16kB	defaultfonts.css
449		text/html	218 bytes	
450	javadl-esd.sun.com	application/xml	3136 bytes	map-1.6.0.xml

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.nyu.edu
- 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 nyu.edu
- Export HTTP objects and note the files that were transferred

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.