Packet Analysis

By Andrew Shi

Packet Analysis

- Packet Analysis is the interpretation of the traffic that occurs in a network
  - You can analyze both captured and live network traffic
  - Difficulty in differentiating between normal traffic vs. abnormal traffic
- Good for troubleshooting
  - Investigate at the “microscopic” level
- Essential for network traffic analysis
  - Spot communication patterns in order to detect and respond to security threats

Packet Analysis

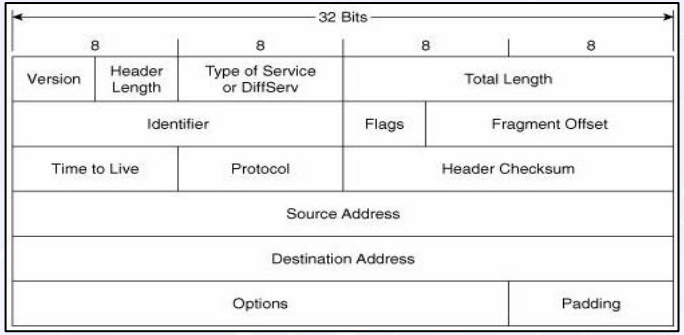
- Packet Analysis can be crucial in identifying the stages of the Cyber Kill Chain
- By identifying these stages, it becomes easier to defend against an attacker at different stages of the Kill Chain

Packets & Protocols

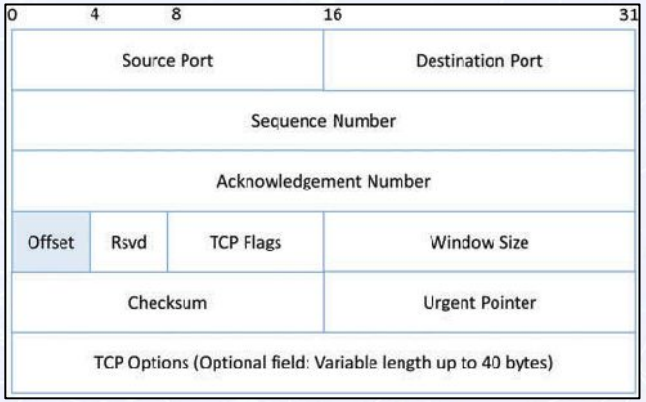
- Packets are small amounts of data sent over a network, such as a LAN or WAN
  - (Header) Source & Destination
  - (Payload) Actual data being transferred
- Upon reaching their destination, Packets reassemble into a single file or other contiguous blocks of data
- Transfers data reliably and efficiently –
  - Large single block of data vs. single block of data
  - Only dropped packets are resent
  - Adapts to network congestion

Packets & Protocols

- Headers:
  - Information about the packet
    - Source
    - Destination
- Different structure depending on protocols
- (Network) Protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices can communicate regardless of the differences in their underlying infrastructures, designs or standards.



IP Header

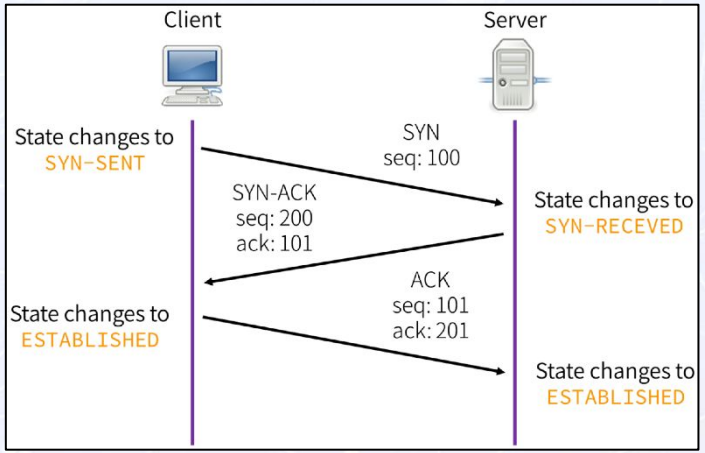


TCP Header

Packets & Protocols

TCP (Transmission Control Protocol)

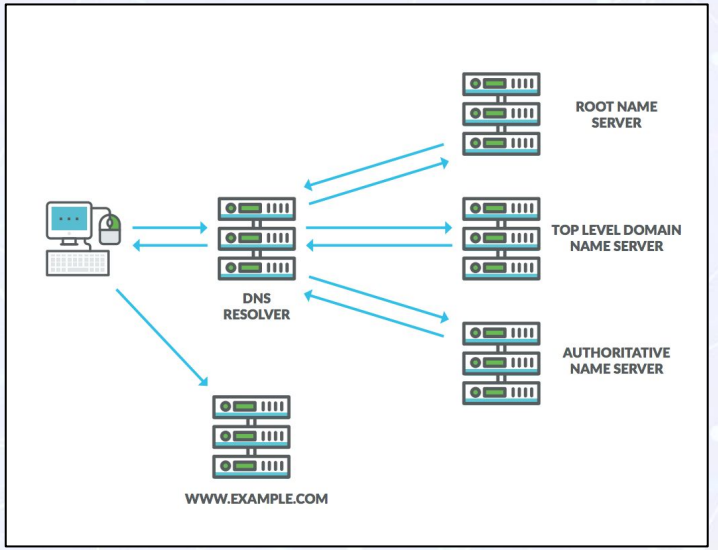
- A standard that defines how to establish and maintain a network conversation; uses a three-way handshake
- Three-way handshake:
  - Stable connection
  - Reliable connection



Packets & Protocols

DNS (Domain Name System)

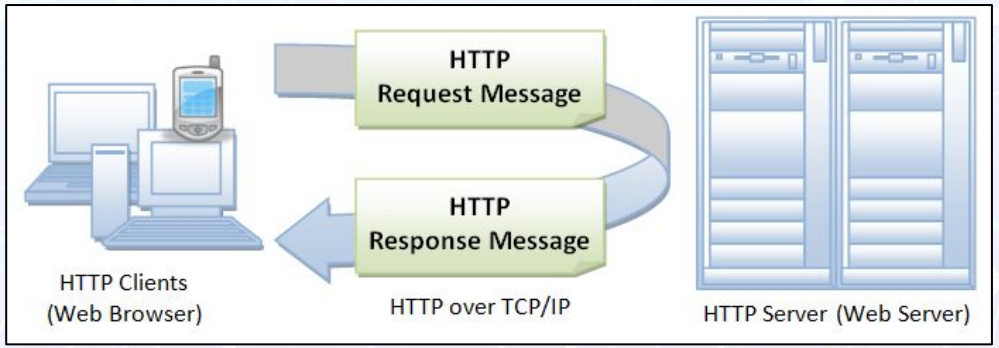
- The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.
- Associates domain names with their IP address
  - www.google.com = 172.217.3[.]110



Packets & Protocols

HTTP (HyperText Transfer Protocol)

- HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
- GET request – request msg
- POST request – response msg



Packet Sniffing

- Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass through a computer network, regardless of how the packet is addressed.
- It's illegal to intercept electronic communication ... unless

> Section 18 U.S. Code § 2511 (2) (a) (i) says:
>
> It shall not be unlawful ... to intercept ... while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service

- Attackers (illegally) and Defenders (legally) sniff packets

Sniffing Tools

Network Mapper (Nmap)

- A network analyzer that is primarily used for port scanning and host discovery
  - Enables connecting to an open port of a live host to capture and analyze their network traffic
- $ nmap

Tcpdump

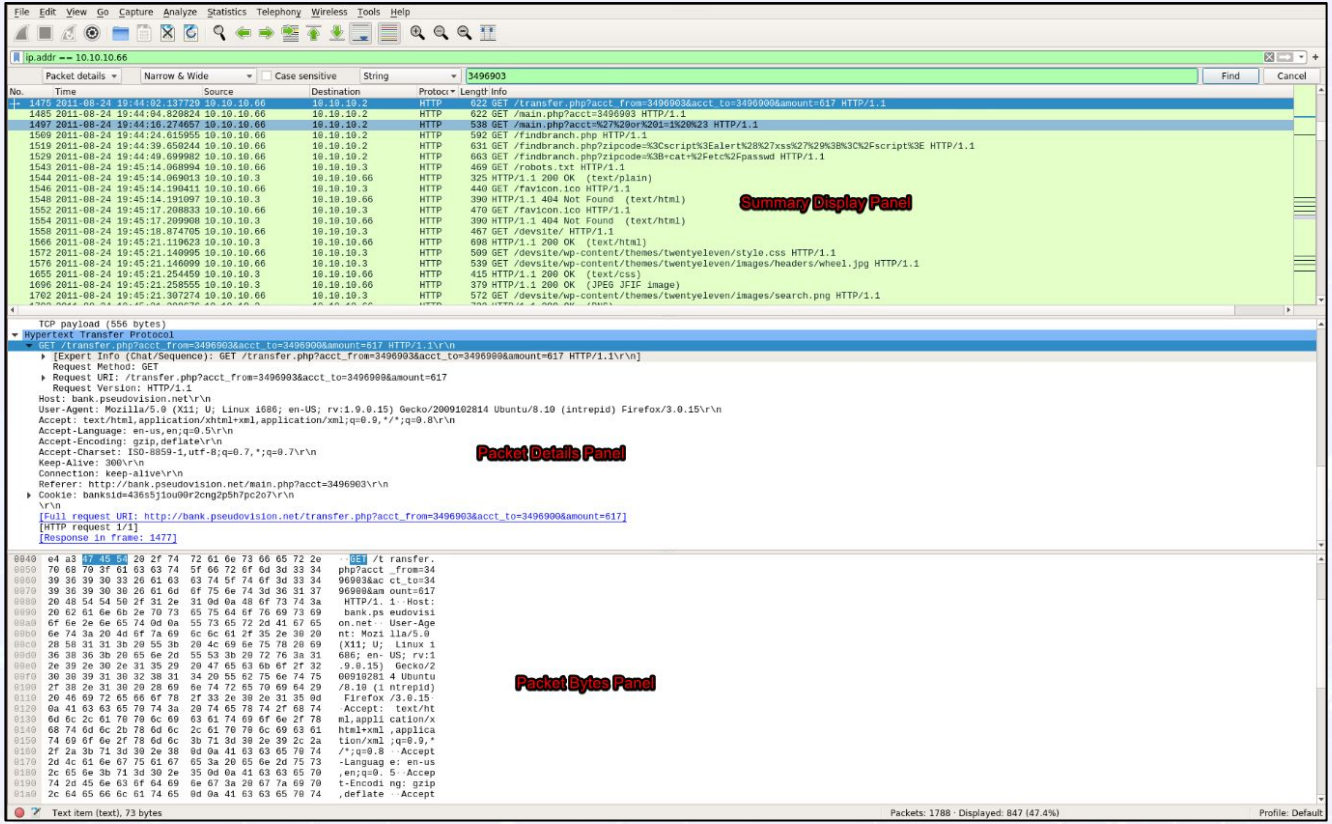
- A packet analyzer that is primarily used for capturing and reading packets
- Prints output to the terminal or to a packet capture (pcap) file
- $ tcpdump

Wireshark

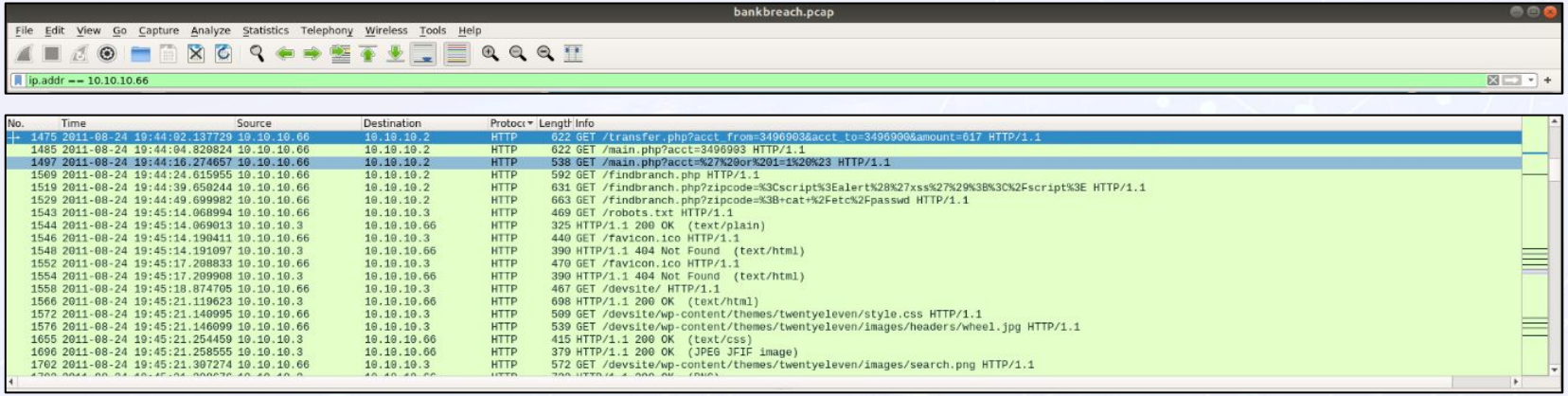
"Wireshark is the world's foremost and widely-used network protocol analyzer."

- Wireshark.org

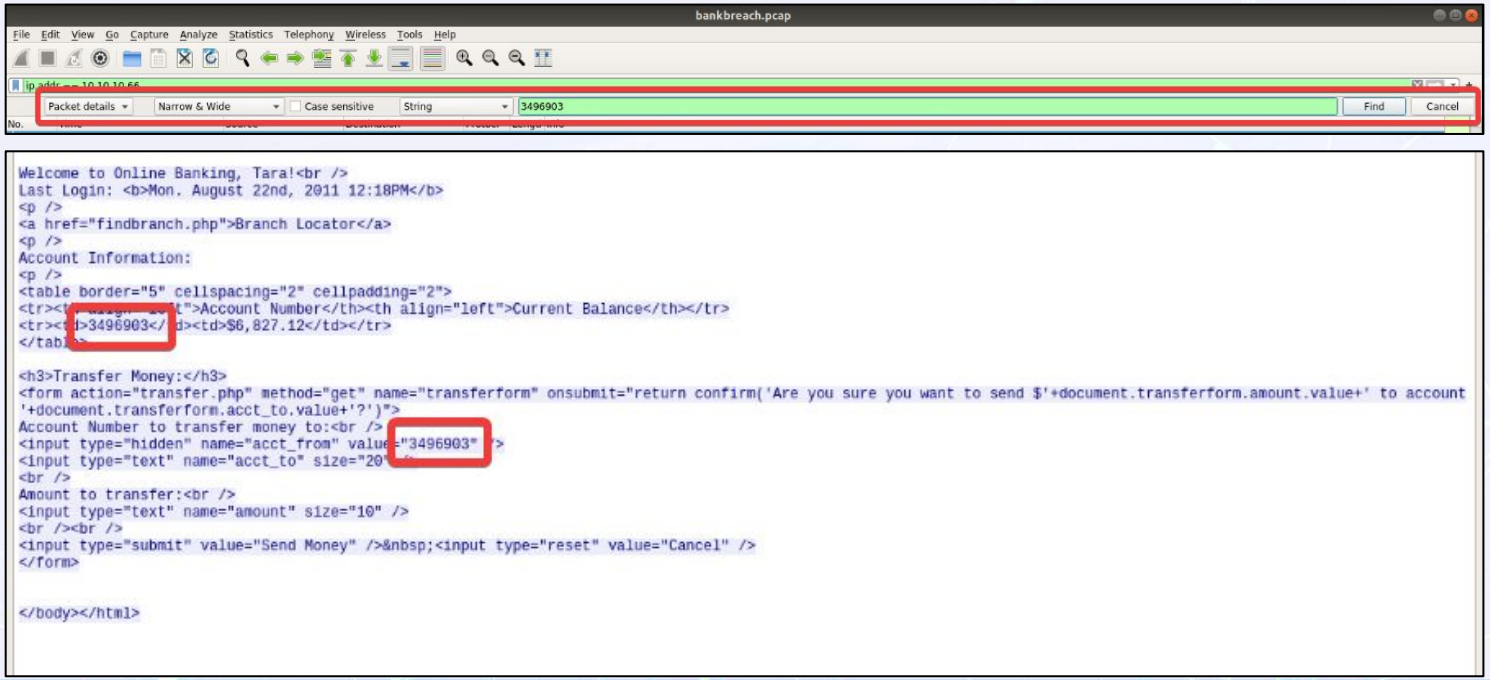
- Same functionality as tcpdump but with a nice GUI
- Includes useful features such as :
  - Sorting & filtering
  - Customizable column display
  - Color coding


Summary Display Panel
Packet Details Panel
Packet Bytes Panel

Wireshark


bankbreach.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.10.10.66
No. Time Source Destination Protocol Length Info
1475 2011-08-24 19:44:02.137729 10.10.10.66 10.10.10.2 HTTP 622 GET /transfer.php?acct_from=3496903&acct_to=3496900&amount=617 HTTP/1.1
1485 2011-08-24 19:44:04.820824 10.10.10.66 10.10.10.2 HTTP 622 GET /main.php?acct=3496903 HTTP/1.1
1497 2011-08-24 19:44:16.274657 10.10.10.66 10.10.10.2 HTTP 538 GET /main.php?acct=%27%20or%201=1%20%23 HTTP/1.1
1509 2011-08-24 19:44:24.615955 10.10.10.66 10.10.10.2 HTTP 592 GET /findbranch.php HTTP/1.1
1519 2011-08-24 19:44:39.650244 10.10.10.66 10.10.10.2 HTTP 631 GET /findbranch.php?zipcode=%3Cscript%3Ealert%28%27xss%27%29%3B%3C%2Fscript%3E HTTP/1.1
1529 2011-08-24 19:44:49.699982 10.10.10.66 10.10.10.2 HTTP 663 GET /findbranch.php?zipcode=%3B+cat+%2Fetc%2Fpasswd HTTP/1.1
1543 2011-08-24 19:45:14.068994 10.10.10.66 10.10.10.3 HTTP 469 GET /robots.txt HTTP/1.1
1544 2011-08-24 19:45:14.069013 10.10.10.3 10.10.10.66 HTTP 325 HTTP/1.1 200 OK (text/plain)
1546 2011-08-24 19:45:14.190411 10.10.10.66 10.10.10.3 HTTP 440 GET /favicon.ico HTTP/1.1
1548 2011-08-24 19:45:14.191097 10.10.10.3 10.10.10.66 HTTP 390 HTTP/1.1 404 Not Found (text/html)
1552 2011-08-24 19:45:17.208833 10.10.10.66 10.10.10.3 HTTP 470 GET /favicon.ico HTTP/1.1
1554 2011-08-24 19:45:17.209908 10.10.10.3 10.10.10.66 HTTP 390 HTTP/1.1 404 Not Found (text/html)
1558 2011-08-24 19:45:18.874705 10.10.10.66 10.10.10.3 HTTP 467 GET /devsite/ HTTP/1.1
1566 2011-08-24 19:45:21.119623 10.10.10.3 10.10.10.66 HTTP 698 HTTP/1.1 200 OK (text/html)
1572 2011-08-24 19:45:21.140995 10.10.10.66 10.10.10.3 HTTP 509 GET /devsite/wp-content/themes/twentyeleven/style.css HTTP/1.1
1576 2011-08-24 19:45:21.146099 10.10.10.66 10.10.10.3 HTTP 539 GET /devsite/wp-content/themes/twentyeleven/images/headers/wheel.jpg HTTP/1.1
1655 2011-08-24 19:45:21.254459 10.10.10.3 10.10.10.66 HTTP 415 HTTP/1.1 200 OK (text/css)
1696 2011-08-24 19:45:21.258555 10.10.10.3 10.10.10.66 HTTP 379 HTTP/1.1 200 OK (JPEG JFIF image)
1702 2011-08-24 19:45:21.307274 10.10.10.66 10.10.10.3 HTTP 572 GET /devsite/wp-content/themes/twentyeleven/images/search.png HTTP/1.1

Wireshark

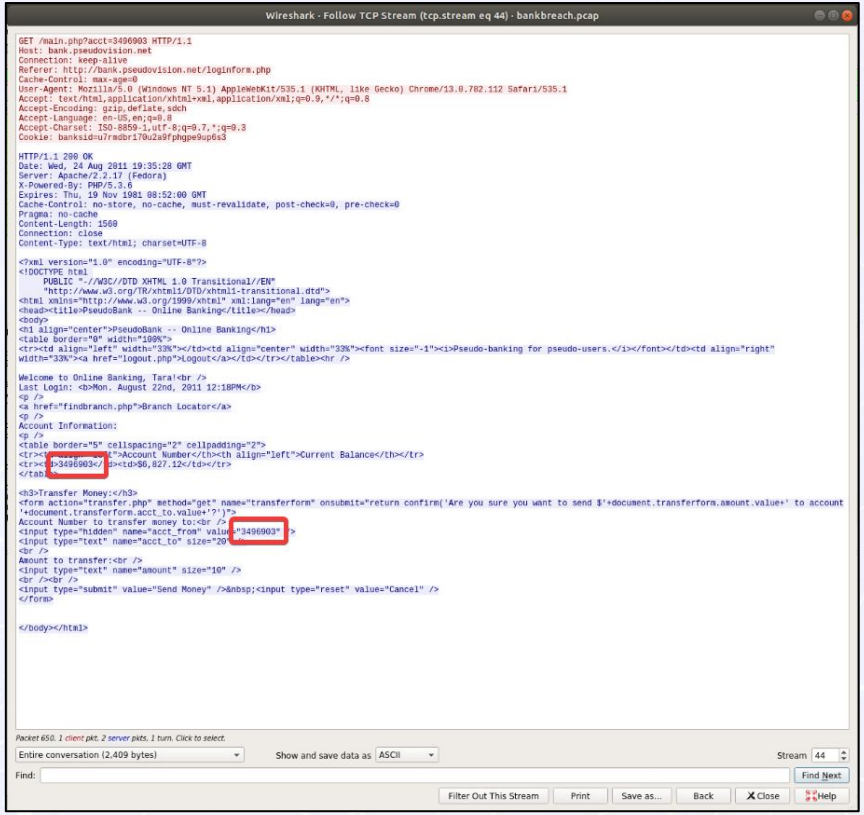

bankbreach.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet details
Narrow & Wide
Case sensitive
String
3496903
Find
Cancel
Welcome to Online Banking, Tara!
Last Login: Mon. August 22nd, 2011 12:18PM
<p />
Branch Locator
<p />
Account Information:
<p />
<table border="5" cellspacing="2" cellpadding="2">
<tr><th align="left">Account Number</th><th align="left">Current Balance</th></tr>
<tr><td>3496903</td><td>$6,827.12</td></tr>
</table>
<h3>Transfer Money:</h3>
<form action="transfer.php" method="get" name="transferform" onsubmit="return confirm('Are you sure you want to send $'+document.transferform.amount.value+' to account
'+document.transferform.acct_to.value+'?')">
Account Number to transfer money to:
<input type="hidden" name="acct_from" value="3496903" />
<input type="text" name="acct_to" size="20" />

Amount to transfer:
<input type="text" name="amount" size="10" />

<input type="submit" value="Send Money" /> <input type="reset" value="Cancel" />
</form>
</body></html>

Wireshark

- Follow TCP and HTTP stream
  - Right-click > Follow > TCP stream
    Right-click > Follow > HTTP stream
- A stream displays all packet details from beginning to end of one exchange
  - The example shows a TCP stream of packets #1460-1471



Snort

- Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS)
- Snort has three modes:
  - Sniffer Mode
    - Read network packets and displays them on the console
  - Packet Logger Mode
    - Save capture data
  - Network Intrusion Detection System Mode
    - Monitor network traffic and analyze it against a rule set defined by the user and perform specific actions based on identified threat

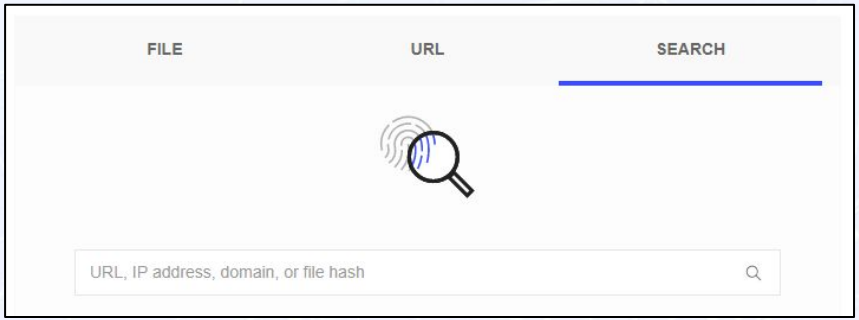
Zeek (Bro)

"Zeek (formerly Bro) is the world's leading platform for network security monitoring. Flexible, open source, and powered by defenders." - zeek.org

- Zeek is an open source network traffic analyzer
- Functions as an IDS but with additional live analysis of network events
- Most immediate benefit is to produce an extensive set of logs such as:
  - conn.log, dns.log, ftp.log, http.log, files.log, ssh.log, weird.log

VirusTotal and Google

- VirusTotal is an online service that analyzes files and URLs enabling the detection of viruses, worms, trojans and other kinds of malicious content using antivirus engines and website scanners
  - Analyzes:
    - Files
    - URLs
    - IP addresses
    - File hashes



VirusTotal and Google

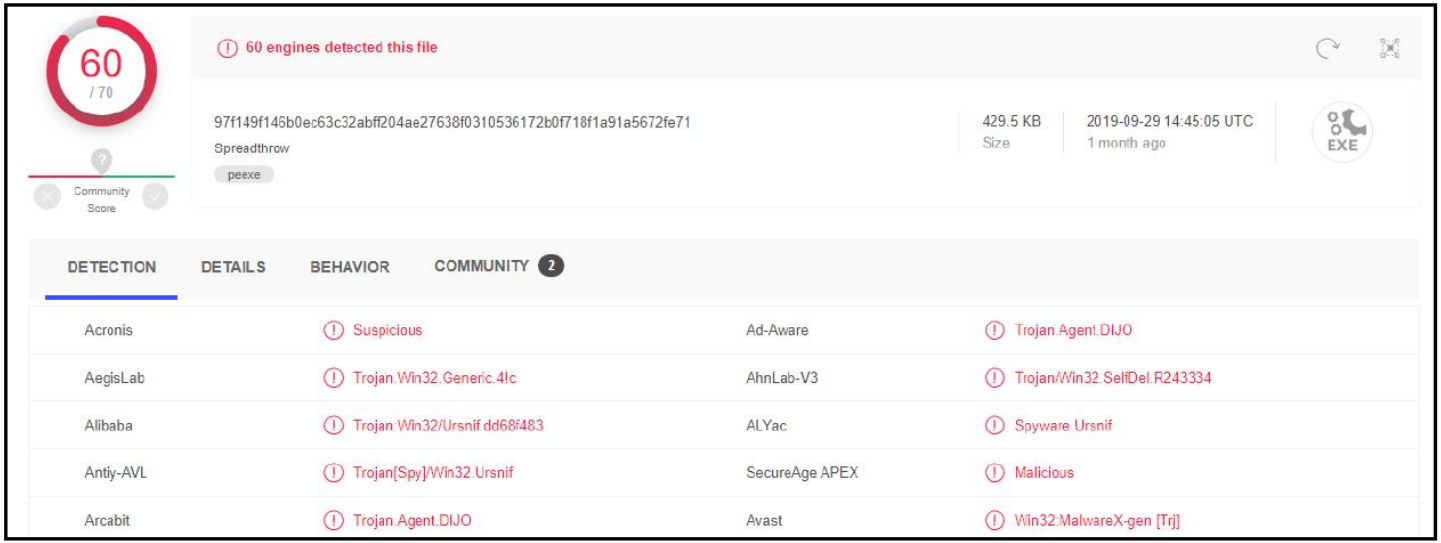
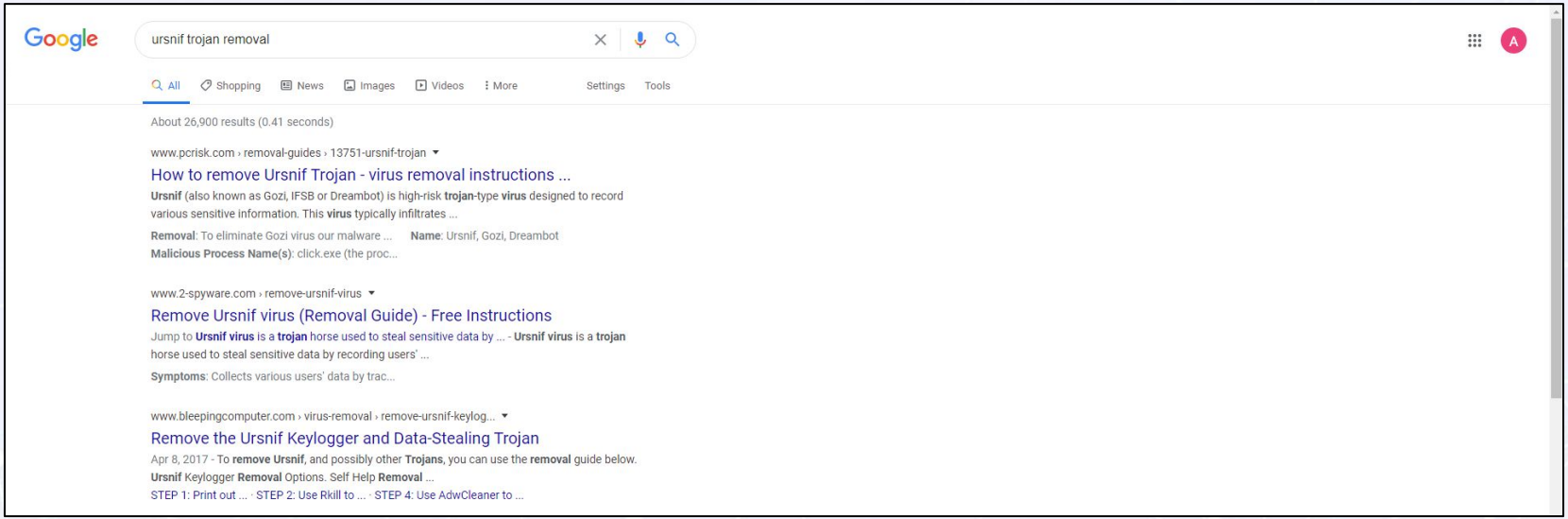


Figure 6: Virus Total results of the malicious object

VirusTotal and Google

- Consult Google for recommended remediation steps and clean up procedures



Break Time

Packet Analysis > Packets & Protocols > Packet Sniffing > Wireshark > Snort > Zeek > VirusTotal & Google > **Break** > Demo & HW

Kahoot

Packet Analysis > Packets & Protocols > Packet Sniffing > Wireshark > Snort > Zeek > VirusTotal & Google > **Break** > Demo & HW

Demo & HW

Objectives:

- Learn to open .pcap files on Wireshark
- Generate Snort alerts
- Familiarize with Wireshark features such as filtering, sorting, searching, and following
- Understand homework expectations

Packet Analysis > Packets & Protocols > Break > Packet Sniffing > Wireshark > Snort > Zeek > VirusTotal & Google > **Demo & HW**

Slide Title

Slide Title

Product A

- Feature 1
- Feature 2
- Feature 3

Product B

- Feature 1
- Feature 2
- Feature 3

Slide Title

- Make Effective Presentations
- Using Awesome Backgrounds
- Engage your Audience
- Capture Audience Attention