NOVEMBER 1 – 2

TexSAW

2019

9th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

Introduction to Digital Forensics

Stephen Ballenger, Nick Ramos, Hailey Gage, Xavier Cadot, and Evelyn Wong

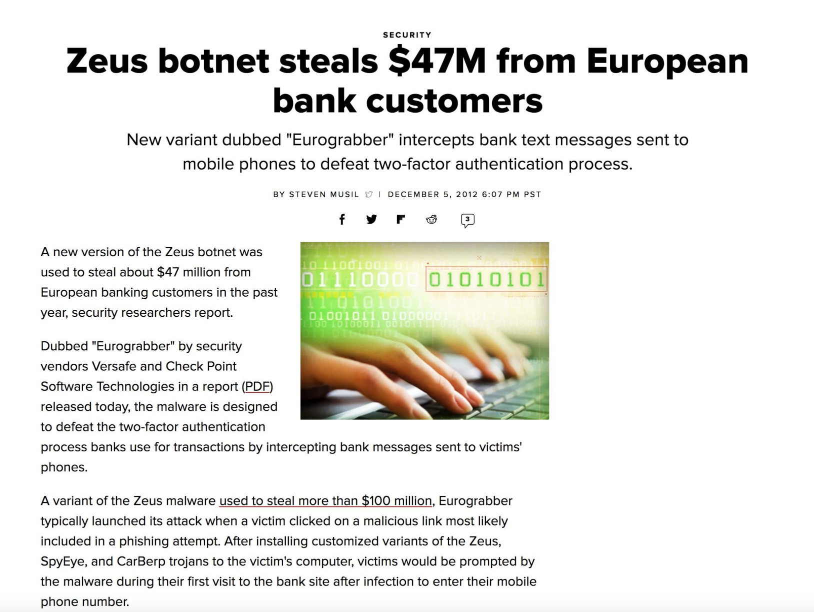
Digital Forensics Overview

- Digital forensics is defined as the process of identifying, extracting, preserving, analyzing, interpreting, and documenting digital evidence (computer data)
- Three primary steps:
  a. Data Collection
  b. Examination & Analysis
  c. Reporting

Source: Rocky Mountain

What is Digital Forensics Used For?

- Corporate or institutional incidents
  - Investigating cyber-attacks or malicious activity on an organization or network
  - Discovering data breaches and mitigating
  - Ex: Zeus botnet was used to steal $47M from European bank customers
  - Ex: How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History



SECURITY

Zeus botnet steals $47M from European bank customers

New variant dubbed "Eurograbber" intercepts bank text messages sent to mobile phones to defeat two-factor authentication process.

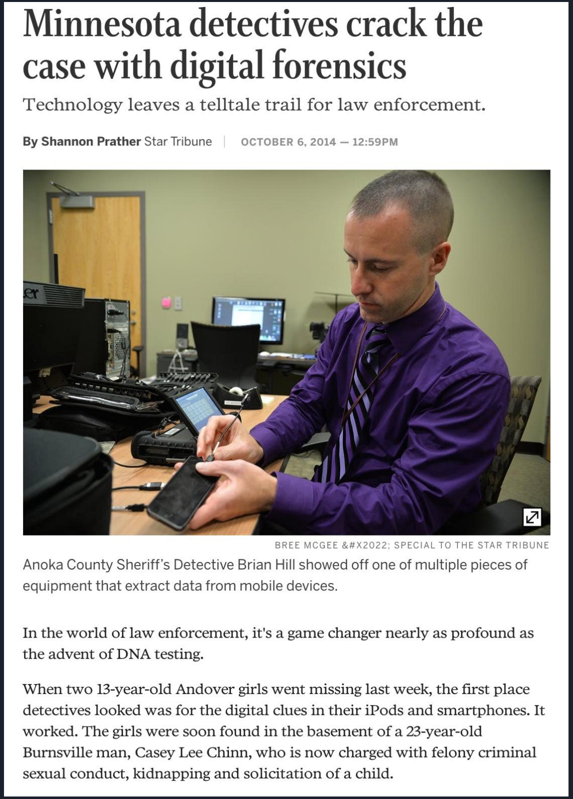
BY STEVEN MUSIL | DECEMBER 5, 2012 6:07 PM PST

A new version of the Zeus botnet was used to steal about $47 million from European banking customers in the past year, security researchers report.

Dubbed "Eurograbber" by security vendors Versafe and Check Point Software Technologies in a report (PDF) released today, the malware is designed to defeat the two-factor authentication process banks use for transactions by intercepting bank messages sent to victims' phones.

A variant of the Zeus malware used to steal more than $100 million, Eurograbber typically launched its attack when a victim clicked on a malicious link most likely included in a phishing attempt. After installing customized variants of the Zeus, SpyEye, and CarBerp trojans to the victim's computer, victims would be prompted by the malware during their first visit to the bank site after infection to enter their mobile phone number.

What is Digital Forensics Used For?



Minnesota detectives crack the case with digital forensics

Technology leaves a telltale trail for law enforcement.

By Shannon Prather Star Tribune | OCTOBER 6, 2014 — 12:59PM

BREE MCGEE &#X2022; SPECIAL TO THE STAR TRIBUNE

Anoka County Sheriff's Detective Brian Hill showed off one of multiple pieces of equipment that extract data from mobile devices.

In the world of law enforcement, it's a game changer nearly as profound as the advent of DNA testing.

When two 13-year-old Andover girls went missing last week, the first place detectives looked was for the digital clues in their iPods and smartphones. It worked. The girls were soon found in the basement of a 23-year-old Burnsville man, Casey Lee Chinn, who is now charged with felony criminal sexual conduct, kidnapping and solicitation of a child.

- Various "real" criminal activity such as fraud, drug trafficking, or child pornography
  - EX: Shelton police seized digital assets from Shelton Finance Department as part of their fraud investigation
  - EX: Minnesota police find missing girls and arrest abductor using data from the girls' cell-phones and iPods

What is Digital Forensics Used For?

- Researchers may analyze forensic data to understand entry points and exploits used by attackers to prevent future events

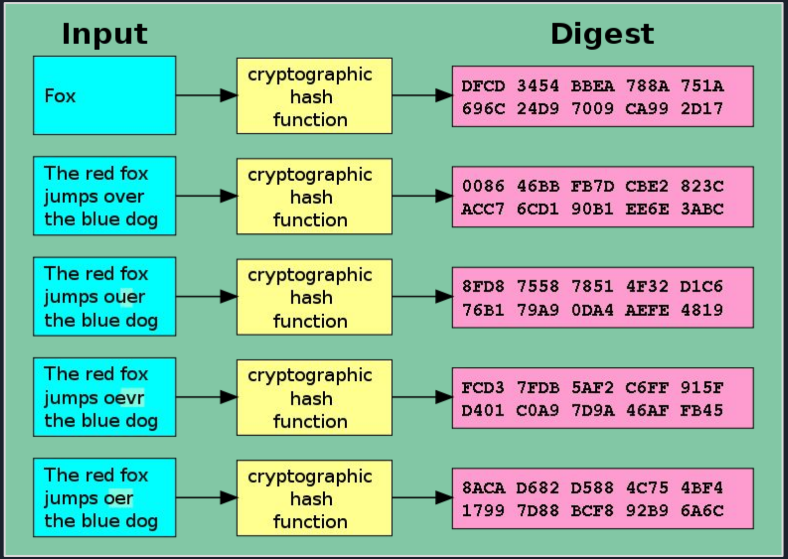
Disclaimer: There is an entire book's worth of information for properly formulating findings from a forensic investigation to stand up in court, but we won't cover that here.

The Three A’s of Digital Forensics

- **Acquire** the evidence without altering or damaging the original data
  - Use a writes blocker
  - Mount disk partitions as read-only
  - Make a clone of the data
    - e.g. > dd if=/dev/sda of=image/sda_clone

The Three A’s of Digital Forensics

- **Authenticate** that the recovered evidence is the same as the original
  - Take a hash of the data using a cryptographic hash function
    - SHA-256, MD5
  - If any of the data is modified, the hash will change significantly



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

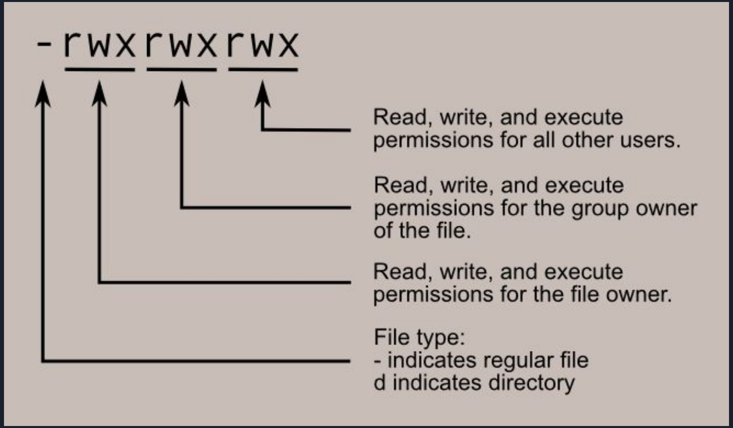
The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Demo: Hashing Files

The Three A’s of Digital Forensics

- **Analyze** the data without modifying it
  - Disable write permissions for the data to prevent modification during analysis
    - Ex: *chmod -w <file>*
  - See file permissions using *ls -la*



Read, write, and execute permissions for all other users.

Read, write, and execute permissions for the group owner of the file.

Read, write, and execute permissions for the file owner.

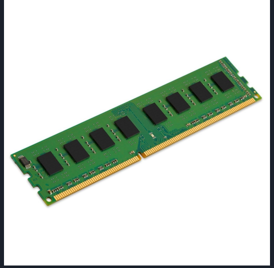
File type:
- indicates regular file
d indicates directory

Demo: File Permissions

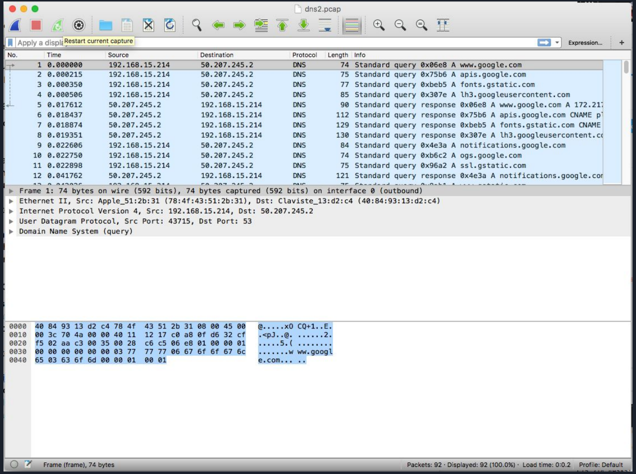
Pop-Quiz #1

What sources of information might someone look at to gather data for a forensic investigation?

Acquiring Evidence for Forensic Investigation



- Physical Storage Media
  - Ex: Hard disks, USB sticks, CDs, DVDs
- Memory (Volatile Storage Media)
  - RAM, caches, logs, processes
- Network
  - Packet capture, IDS logs



```
No.  Time      Source          Destination     Protocol Length Info
  1 0.000000  192.168.15.214  50.207.245.2    DNS       74 Standard query 0x06e8 A www.google.com
  2 0.000215  192.168.15.214  50.207.245.2    DNS       75 Standard query 0x75b6 A apis.google.com
  3 0.000350  192.168.15.214  50.207.245.2    DNS       77 Standard query 0xbeb5 A fonts.gstatic.com
  4 0.000506  192.168.15.214  50.207.245.2    DNS       85 Standard query 0x307e A lh3.googleusercontent.com
  5 0.017612  50.207.245.2    192.168.15.214  DNS       90 Standard query response 0x06e8 A www.google.com A 172.21
  6 0.018437  50.207.245.2    192.168.15.214  DNS      112 Standard query response 0x75b6 A apis.google.com CNAME p
  7 0.018874  50.207.245.2    192.168.15.214  DNS      129 Standard query response 0xbeb5 A fonts.gstatic.com CNAME
  8 0.019351  50.207.245.2    192.168.15.214  DNS      130 Standard query response 0x307e A lh3.googleusercontent.co
  9 0.022606  192.168.15.214  50.207.245.2    DNS       84 Standard query 0x4e3a A notifications.google.com
 10 0.022750  192.168.15.214  50.207.245.2    DNS       74 Standard query 0xb6c2 A ogs.google.com
 11 0.022898  192.168.15.214  50.207.245.2    DNS       75 Standard query 0x96a2 A ssl.gstatic.com
 12 0.041762  50.207.245.2    192.168.15.214  DNS      121 Standard query response 0x4e3a A notifications.google.co
```

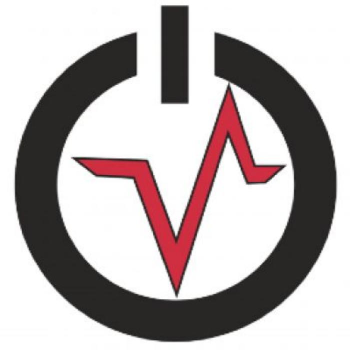
```
▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 (outbound)
▶ Ethernet II, Src: Apple_51:2b:31 (78:4f:43:51:2b:31), Dst: Claviste_13:d2:c4 (40:84:93:13:d2:c4)
▶ Internet Protocol Version 4, Src: 192.168.15.214, Dst: 50.207.245.2
▶ User Datagram Protocol, Src Port: 43715, Dst Port: 53
▶ Domain Name System (query)
```

```
0000  40 84 93 13 d2 c4 78 4f  43 51 2b 31 08 00 45 00   @.....xO CQ+1..E.
0010  00 3c 70 4a 00 00 40 11  12 17 c0 a8 0f d6 32 cf   .<pJ..@. ......2.
0020  f5 02 aa c3 00 35 00 28  c6 c5 06 e8 01 00 00 01   .....5.( ........
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..
```

Frame (frame), 74 bytes   Packets: 92 · Displayed: 92 (100.0%) · Load time: 0:0.2   Profile: Default

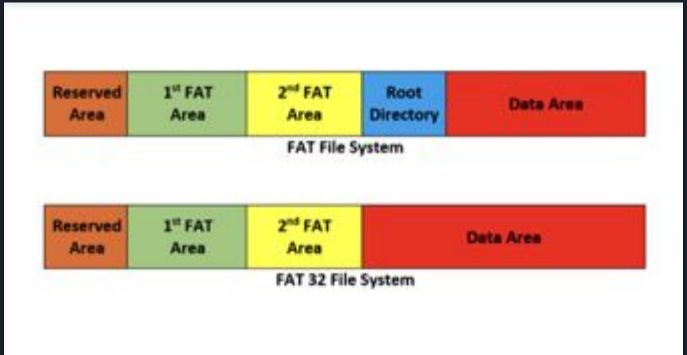
Tools for Analyzing Forensic Data

- Different data sources require different tools for analyzing data:
    - For Hard Disks - Autopsy
    - For Memory - Volatility Framework, Digital Forensic Framework
    - For Network - Wireshark



File System Forensics - Types of File Systems

- FAT, FAT32
  - File Allocation Table
- NTFS
  - New Technology File System
- EXT
  - Extended File System
- Different from File Formats such as .jpg, .pdf, etc.



File System Forensics - Investigation Steps

- Acquisition
- Validation/Discrimination
- Extraction
- Reconstruction
- Reporting

File System Forensics - Acquisition

- System needs to be secured; All files need to be accounted for/copied in most situations
- Four main methods:
  a. Disk-to-Image : most common
  b. Disk-to-Disk : used when Disk-to-Image fails/is not possible
  c. Logical : only captures files of interest. Only used when time is limited
  d. Sparse : gathers fragments of scattered data

File System Forensics - Validation/Discrimination

- Validation is important to ensure the integrity of the copied data
  - Done by taking hashes of both the original disk image and the forensic image copy and comparing to find a match
- If both hashes match, that confirms they are exact copies and can (potentially) be admissible as court evidence

File System Forensics - Extraction

- Process of collecting information
- Deleted files *are not deleted forever* and can be recovered
- Extracting data from unallocated space is called *file carving*
- A file should have a header and a footer somewhere in memory
    - Data between those two points is extracted and analyzed

File System Forensics - Reconstruction

- Not all files will be intact or in one piece
- These files are put back together with tools based on reconstruction algorithms
- Recovered files are then further analyzed

Pop Quiz # 2

What should you document in your report when conducting a Digital Forensic Investigation?

File System Forensics - Reporting

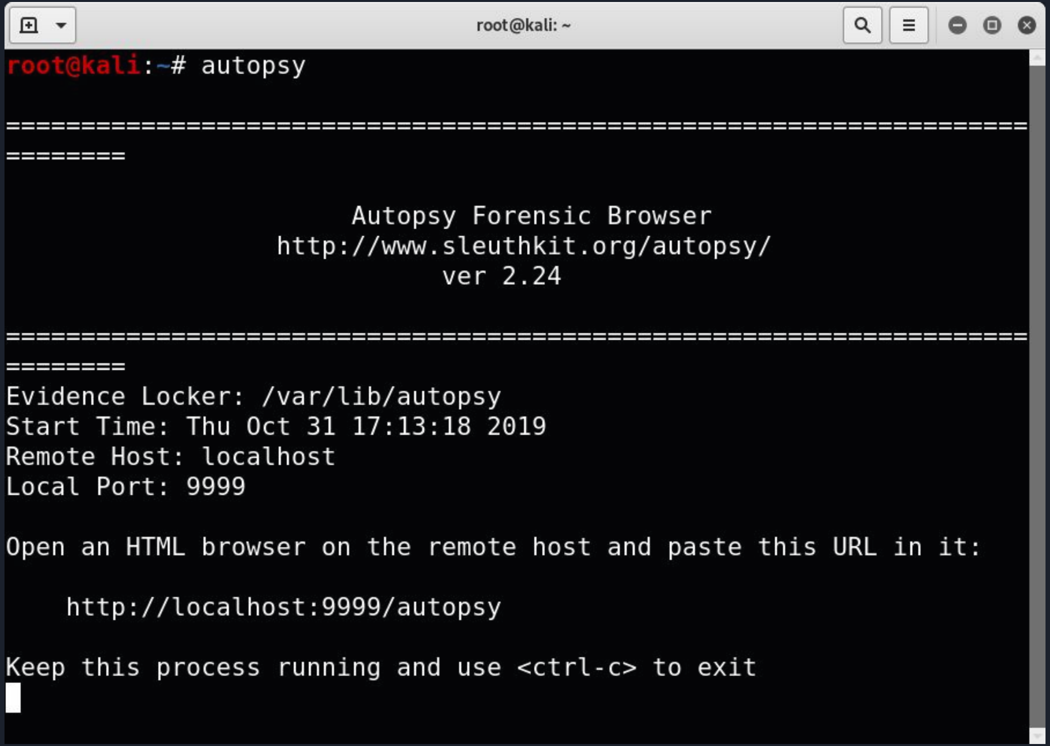
- Report everything!
  - All steps taken
  - All findings

Demo: File System Forensics with Autopsy

Download

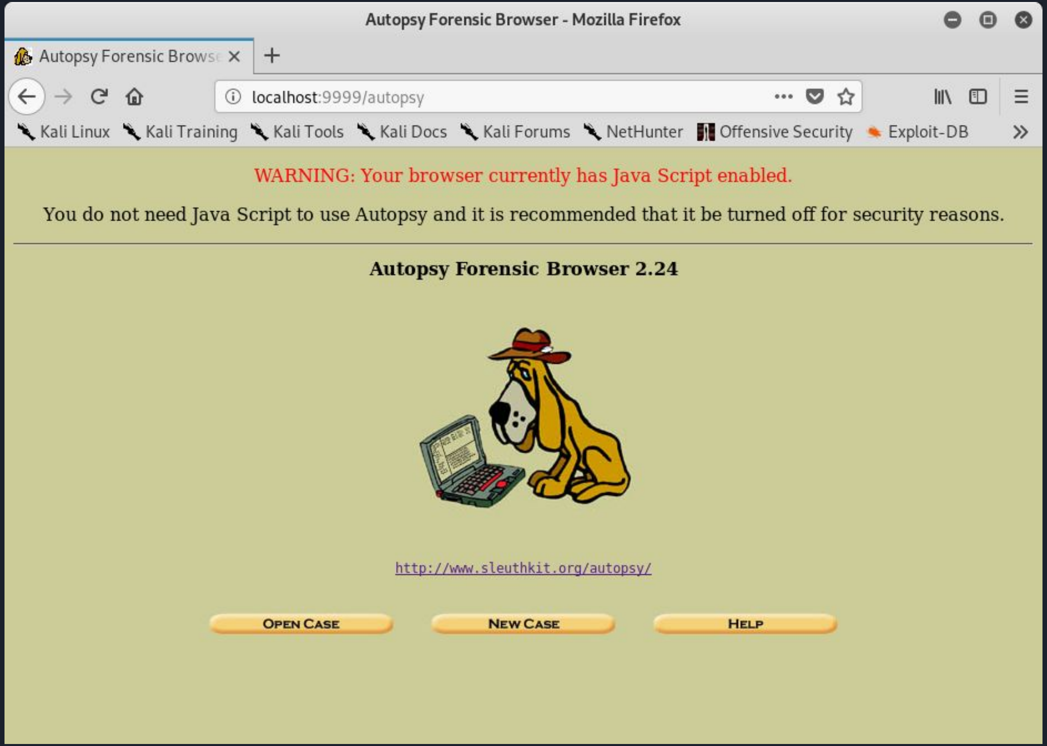
tiny.cc/f0hifz

1. Run autopsy from terminal



```
root@kali:~# autopsy

====================================================================
=========


                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

====================================================================
=========
Evidence Locker: /var/lib/autopsy
Start Time: Thu Oct 31 17:13:18 2019
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

2. Navigate to localhost:9999/autopsy in Firefox



Autopsy Forensic Browser - Mozilla Firefox

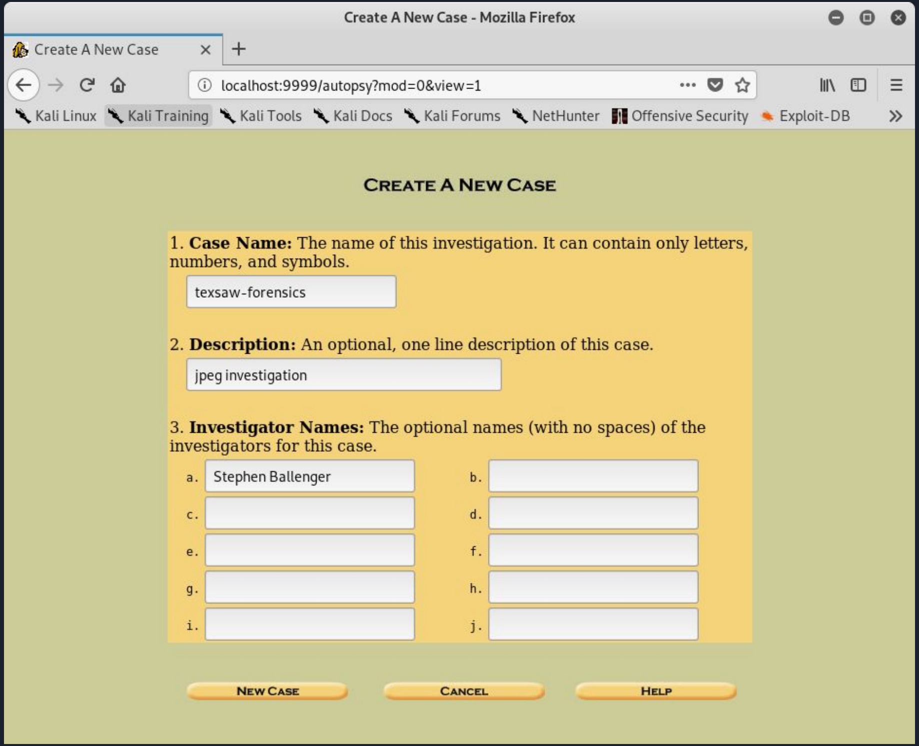
WARNING: Your browser currently has Java Script enabled.

You do not need Java Script to use Autopsy and it is recommended that it be turned off for security reasons.

Autopsy Forensic Browser 2.24

http://www.sleuthkit.org/autopsy/

3. Enter new case information



CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

texsaw-forensics

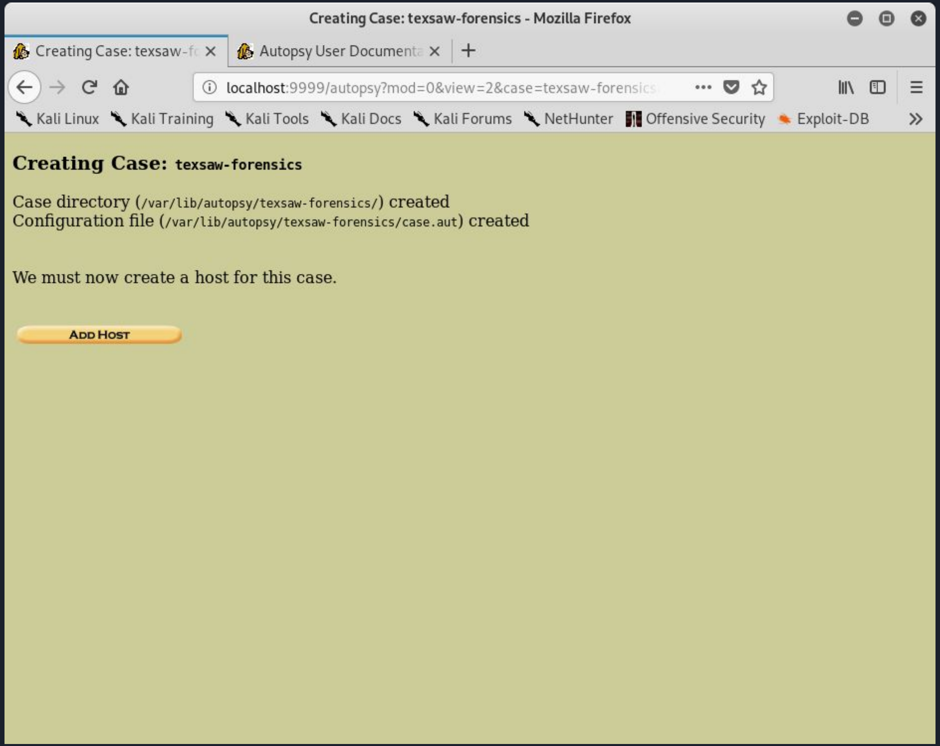
2. **Description:** An optional, one line description of this case.

jpeg investigation

3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Stephen Ballenger
b.
c.
d.
e.
f.
g.
h.
i.
j.

4. Add host

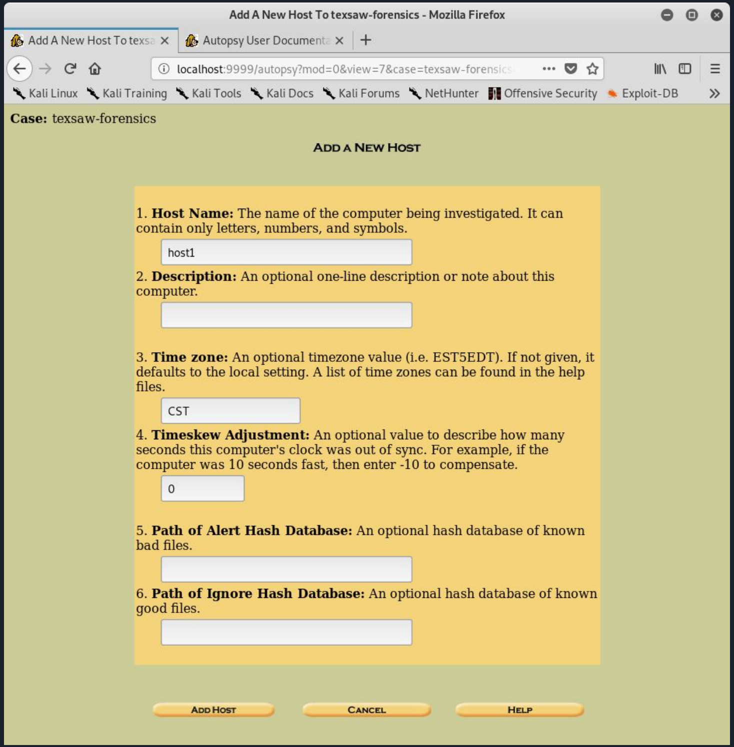


Creating Case: `texsaw-forensics`

Case directory (`/var/lib/autopsy/texsaw-forensics/`) created
Configuration file (`/var/lib/autopsy/texsaw-forensics/case.aut`) created

We must now create a host for this case.

5. Enter new host information



Case: texsaw-forensics

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

host1

2. **Description:** An optional one-line description or note about this computer.

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

CST

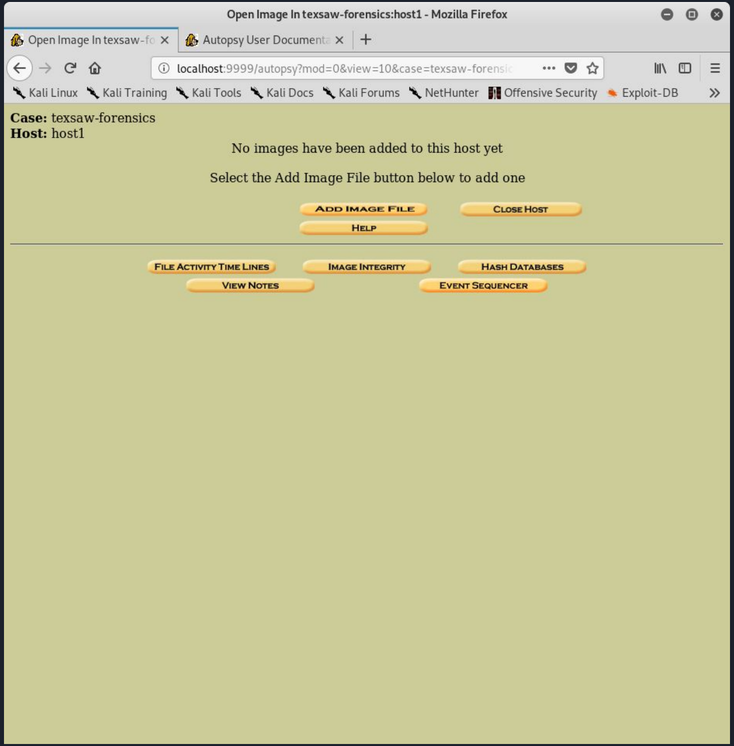
4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

0

5. **Path of Alert Hash Database:** An optional hash database of known bad files.

6. **Path of Ignore Hash Database:** An optional hash database of known good files.

6. Add image file

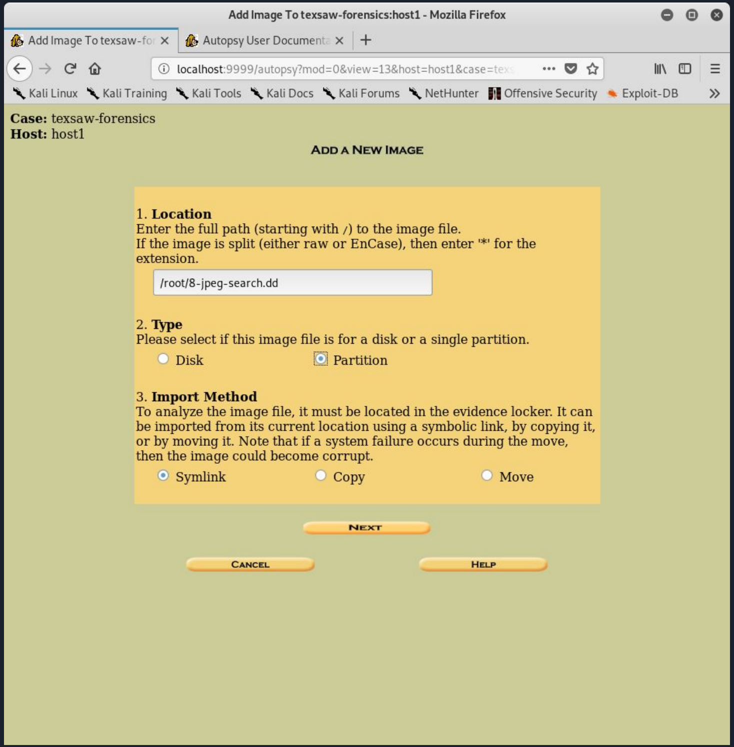


Case: texsaw-forensics
Host: host1

No images have been added to this host yet

Select the Add Image File button below to add one

7. Add image information



Case: texsaw-forensics
Host: host1

ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

/root/8-jpeg-search.dd

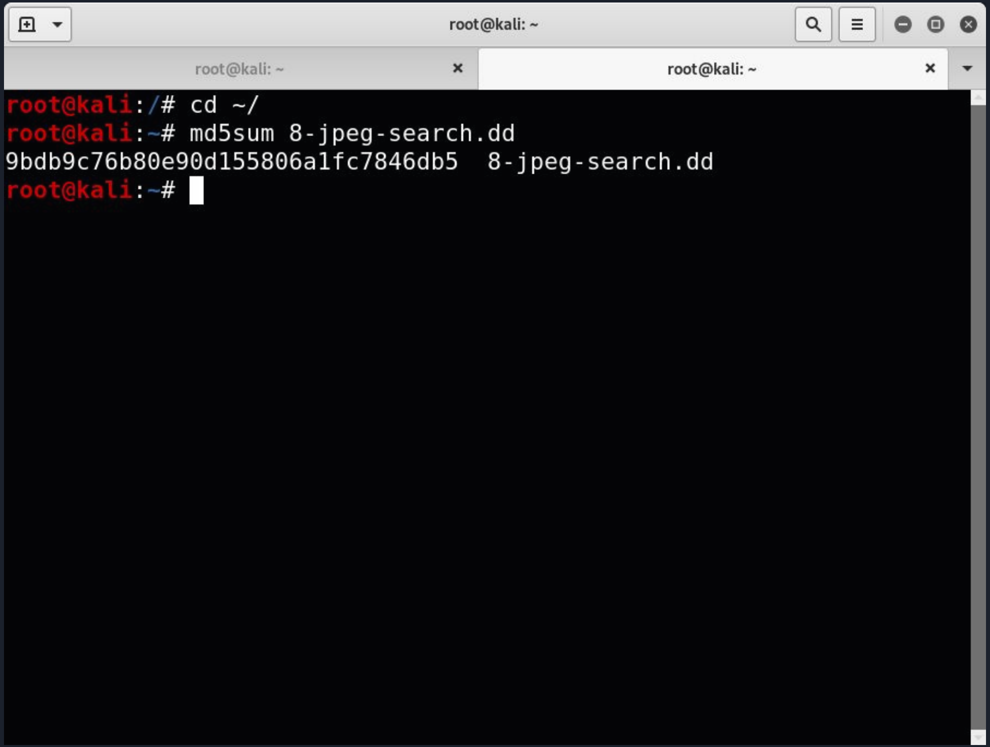
2. **Type**
Please select if this image file is for a disk or a single partition.

○ Disk ● Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.

● Symlink ○ Copy ○ Move

8. Get MD5 hash for image file



```
root@kali:/# cd ~/
root@kali:~# md5sum 8-jpeg-search.dd
9bdb9c76b80e90d155806a1fc7846db5  8-jpeg-search.dd
root@kali:~# 
```

9. Add MD5 hash to Autopsy

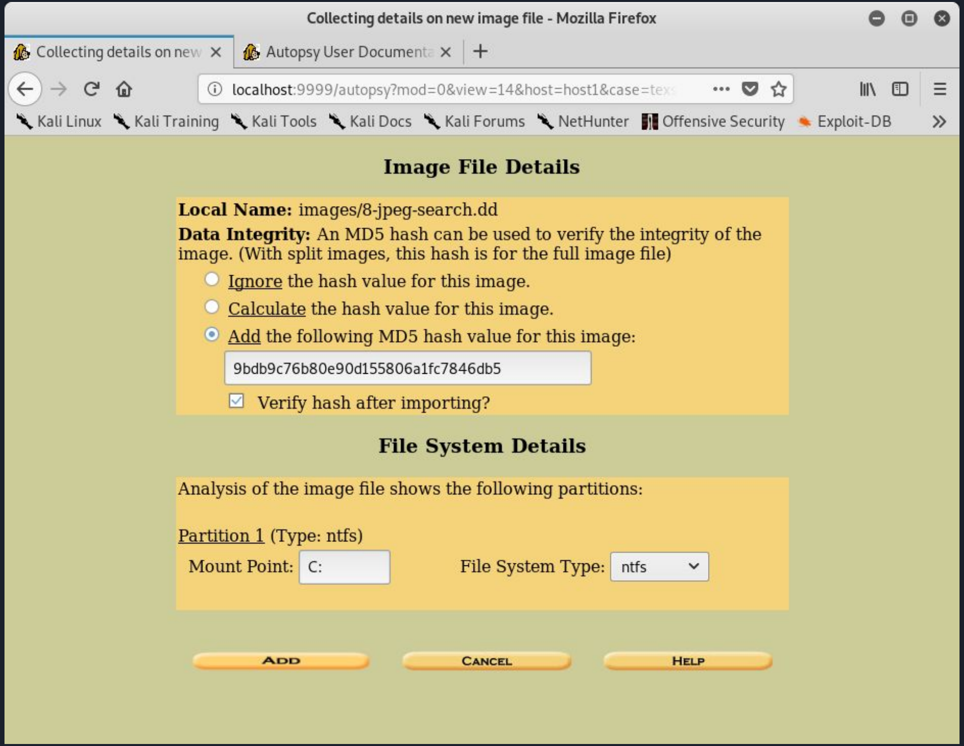

Collecting details on new image file - Mozilla Firefox
Collecting details on new
Autopsy User Documenta
localhost:9999/autopsy?mod=0&view=14&host=host1&case=tex
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
ADD
CANCEL
HELP

Image File Details

Local Name: images/8-jpeg-search.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

○ Ignore the hash value for this image.

○ Calculate the hash value for this image.

● Add the following MD5 hash value for this image:

9bdb9c76b80e90d155806a1fc7846db5

☑ Verify hash after importing?

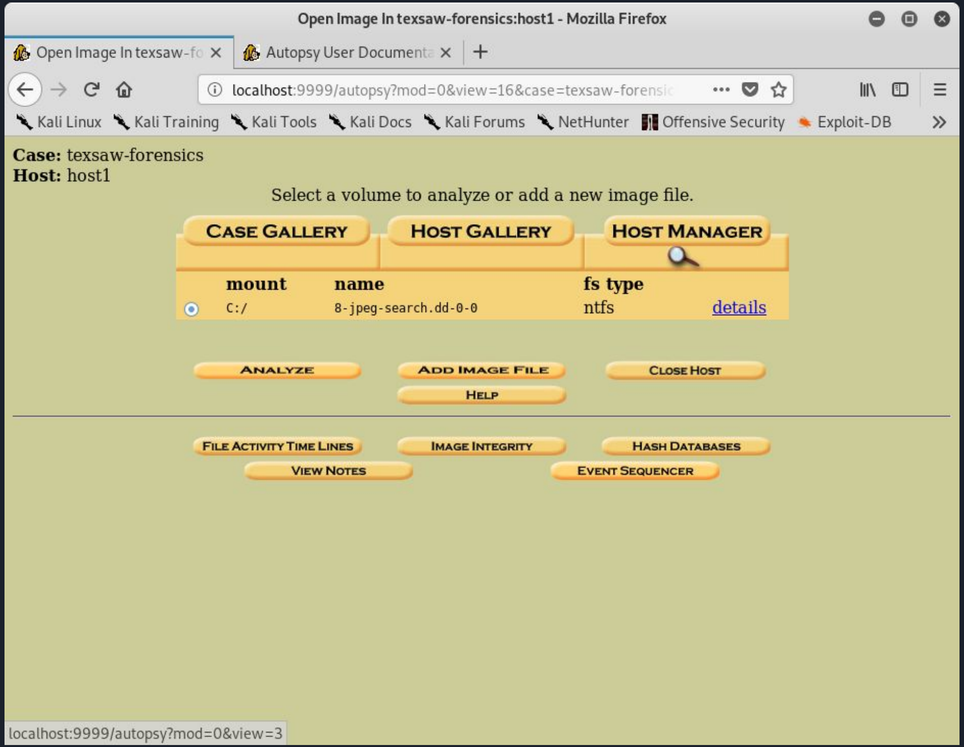
File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: ntfs)

Mount Point: C: File System Type: ntfs

10. Analyze!



Case: texsaw-forensics
Host: host1

Select a volume to analyze or add a new image file.

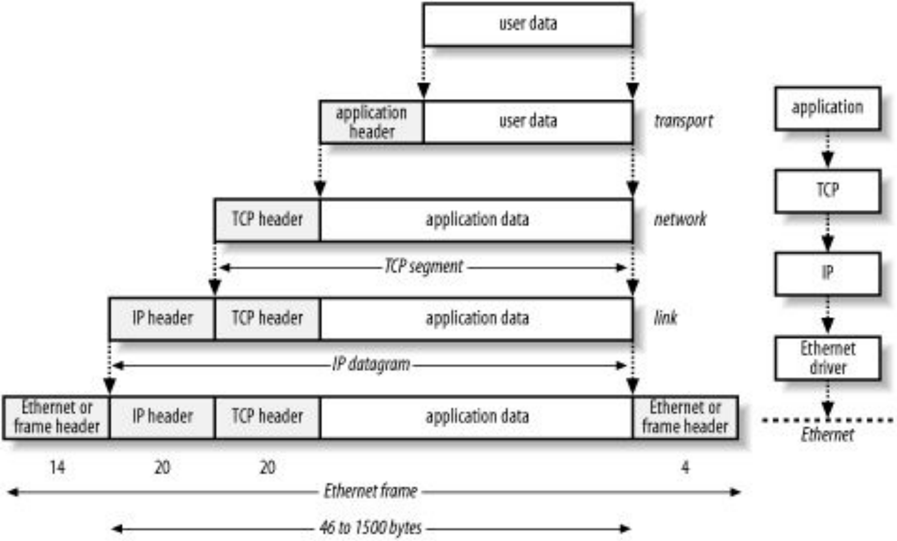
	mount	name	fs type	
●	C:/	8-jpeg-search.dd-0-0	ntfs	details

Network Forensics- Intro

- Branch of digital forensics
- Monitoring and analysis of computer network traffic and log files
- Why?
    - Information gathering
    - Legal evidence
    - Intrusion detection
- Network traffic can be captured via PCAP

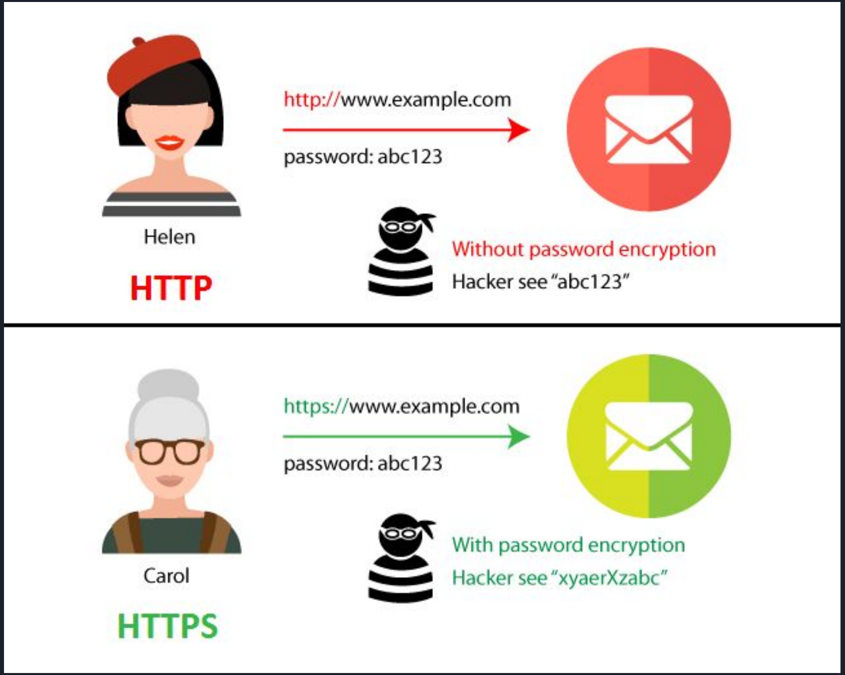
What is a packet?

- A formatted unit of data carried by a network
- Consists of control information and user data, known as the payload
- Packets and networks are layered:
    - Network Access Layer (Ethernet)
    - Internet Layer (IP, ICMP)
    - Transport Layer (TCP, UDP)
    - Application Layer (HTTP, HTTPS, DNS, SMTP)



HTTP vs. HTTPS

- Hypertext Transfer Protocol (HTTP) is primarily used to transfer data from a web server to a browser
- HTTP information is not encrypted, i.e. anyone capturing network traffic can read what is be transmitted
- Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP that is used to secure communication over a network
- Packet data is encrypted using SSL/TLS, public-key cryptographic protocols

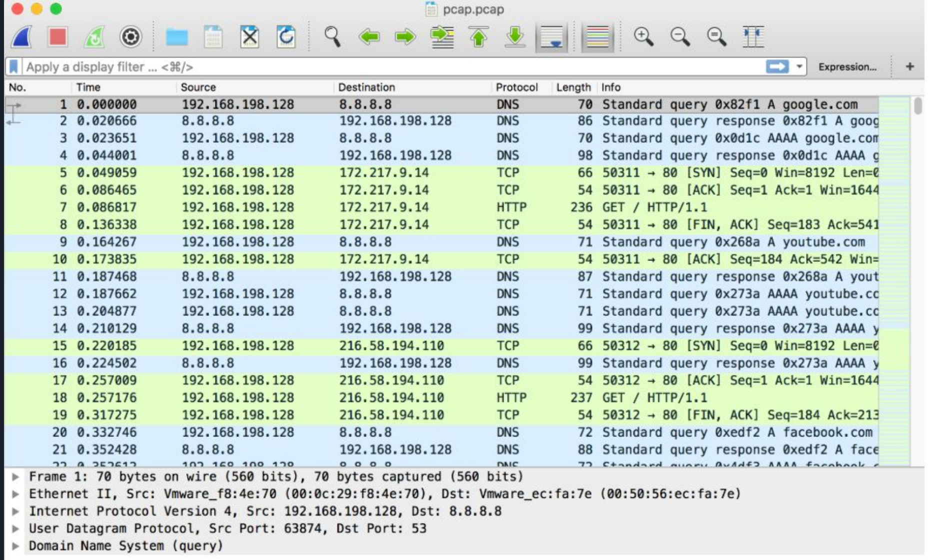


Network Forensics - Tools

- Wireshark
- Kibana
- TcpDump
- Security Onion
    - Bro
    - Suricata
    - OSSEC

Wireshark

- A free, open-source packet analyzer
- Similar to tcpdump, but has a graphical interface and additional sorting and filtering options
- Network interfaces are put into promiscuous mode, allowing them to see all network traffic visible on that interface
- Packets captured can be saved in a .pcap file for later viewing or processing



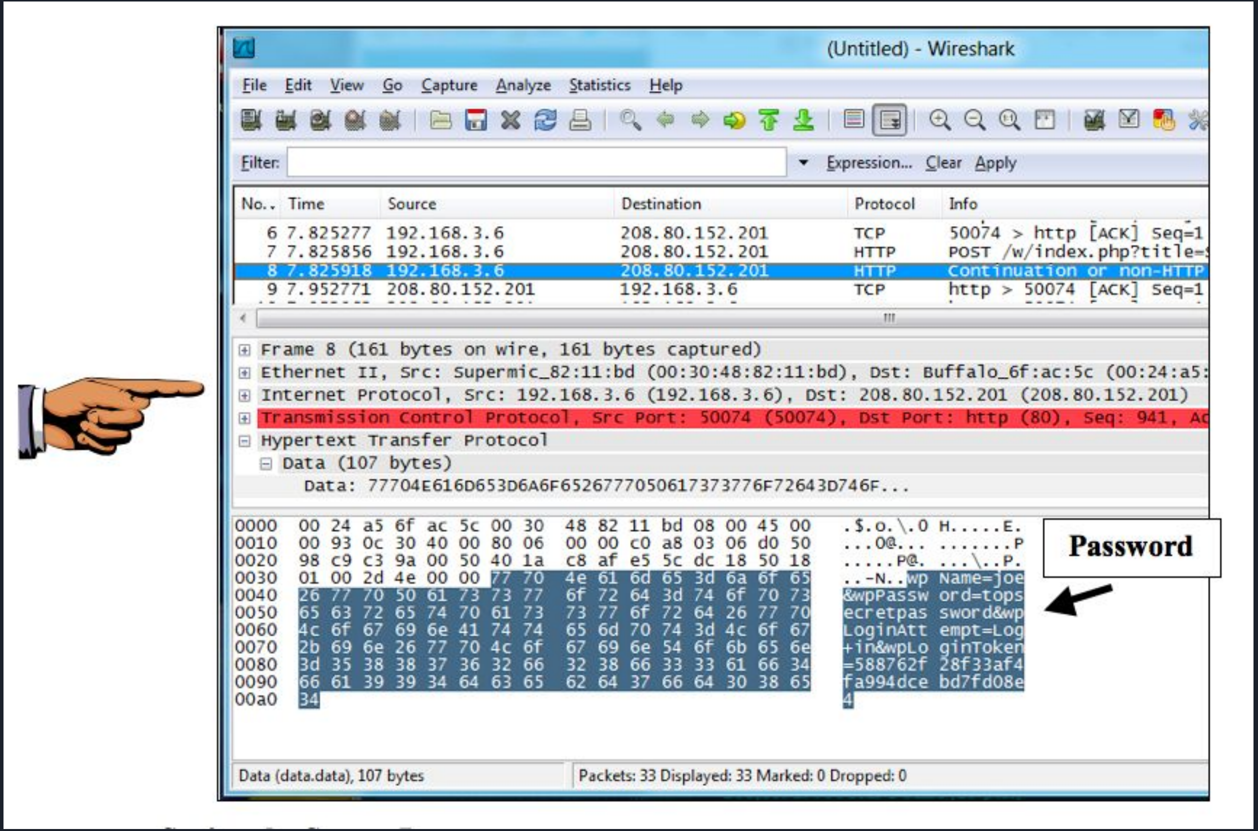
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.198.128	8.8.8.8	DNS	70	Standard query 0x82f1 A google.com
2	0.020666	8.8.8.8	192.168.198.128	DNS	86	Standard query response 0x82f1 A goog
3	0.023651	192.168.198.128	8.8.8.8	DNS	70	Standard query 0x0d1c AAAA google.com
4	0.044001	8.8.8.8	192.168.198.128	DNS	98	Standard query response 0x0d1c AAAA g
5	0.049059	192.168.198.128	172.217.9.14	TCP	66	50311 → 80 [SYN] Seq=0 Win=8192 Len=0
6	0.086465	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [ACK] Seq=1 Ack=1 Win=1644
7	0.086817	192.168.198.128	172.217.9.14	HTTP	236	GET / HTTP/1.1
8	0.136338	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [FIN, ACK] Seq=183 Ack=541
9	0.164267	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x268a A youtube.com
10	0.173835	192.168.198.128	172.217.9.14	TCP	54	50311 → 80 [ACK] Seq=184 Ack=542 Win=
11	0.187468	8.8.8.8	192.168.198.128	DNS	87	Standard query response 0x268a A yout
12	0.187662	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x273a AAAA youtube.cc
13	0.204877	192.168.198.128	8.8.8.8	DNS	71	Standard query 0x273a AAAA youtube.cc
14	0.210129	8.8.8.8	192.168.198.128	DNS	99	Standard query response 0x273a AAAA y
15	0.220185	192.168.198.128	216.58.194.110	TCP	66	50312 → 80 [SYN] Seq=0 Win=8192 Len=0
16	0.224502	8.8.8.8	192.168.198.128	DNS	99	Standard query response 0x273a AAAA y
17	0.257009	192.168.198.128	216.58.194.110	TCP	54	50312 → 80 [ACK] Seq=1 Ack=1 Win=1644
18	0.257176	192.168.198.128	216.58.194.110	HTTP	237	GET / HTTP/1.1
19	0.317275	192.168.198.128	216.58.194.110	TCP	54	50312 → 80 [FIN, ACK] Seq=184 Ack=213
20	0.332746	192.168.198.128	8.8.8.8	DNS	72	Standard query 0xedf2 A facebook.com
21	0.352428	8.8.8.8	192.168.198.128	DNS	88	Standard query response 0xedf2 A face
22	0.352613	192.168.198.128	8.8.8.8	DNS	72	Standard query 0x4df3 AAAA facebook.c

```
▶ Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
▶ Ethernet II, Src: Vmware_f8:4e:70 (00:0c:29:f8:4e:70), Dst: Vmware_ec:fa:7e (00:50:56:ec:fa:7e)
▶ Internet Protocol Version 4, Src: 192.168.198.128, Dst: 8.8.8.8
▶ User Datagram Protocol, Src Port: 63874, Dst Port: 53
▶ Domain Name System (query)
```

Pop Quiz # 3

What happens when Joe logs into a website on a http protocol?

Network Forensics- Joe’s Top Secret Password

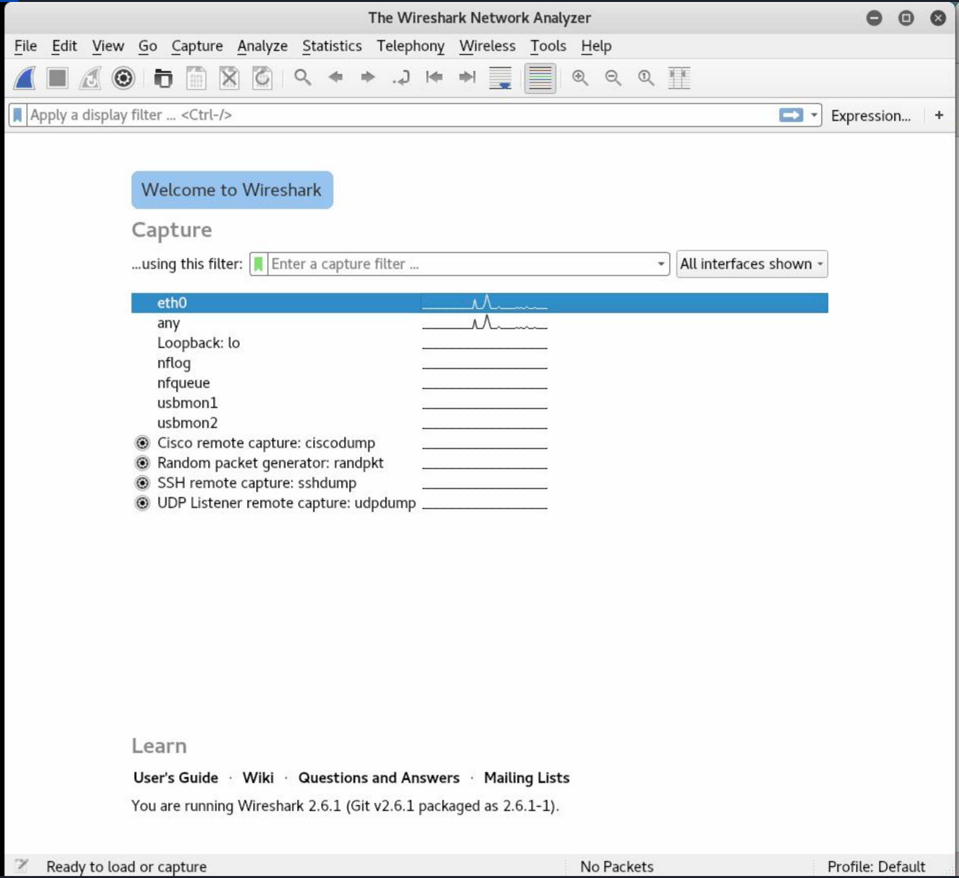

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Password

```
No..  Time      Source           Destination      Protocol  Info
    6 7.825277  192.168.3.6      208.80.152.201   TCP       50074 > http [ACK] Seq=1
    7 7.825856  192.168.3.6      208.80.152.201   HTTP      POST /w/index.php?title=
    8 7.825918  192.168.3.6      208.80.152.201   HTTP      Continuation or non-HTTP
    9 7.952771  208.80.152.201   192.168.3.6      TCP       http > 50074 [ACK] Seq=1
```

```
⊞ Frame 8 (161 bytes on wire, 161 bytes captured)
⊞ Ethernet II, Src: Supermic_82:11:bd (00:30:48:82:11:bd), Dst: Buffalo_6f:ac:5c (00:24:a5:
⊞ Internet Protocol, Src: 192.168.3.6 (192.168.3.6), Dst: 208.80.152.201 (208.80.152.201)
⊞ Transmission Control Protocol, Src Port: 50074 (50074), Dst Port: http (80), Seq: 941, Ac
⊟ Hypertext Transfer Protocol
  ⊟ Data (107 bytes)
      Data: 77704E616D653D6A6F6526777050617373776F72643D746F...
```

```
0000   00 24 a5 6f ac 5c 00 30  48 82 11 bd 08 00 45 00   .$.o.\.0 H.....E.
0010   00 93 0c 30 40 00 80 06  00 00 c0 a8 03 06 d0 50   ...0@... .......P
0020   98 c9 c3 9a 00 50 40 1a  c8 af e5 5c dc 18 50 18   .....P@. ...\..P.
0030   01 00 2d 4e 00 00 77 70  4e 61 6d 65 3d 6a 6f 65   ..-N..wp Name=joe
0040   26 77 70 50 61 73 73 77  6f 72 64 3d 74 6f 70 73   &wpPassw ord=tops
0050   65 63 72 65 74 70 61 73  73 77 6f 72 64 26 77 70   ecretpas sword&wp
0060   4c 6f 67 69 6e 41 74 74  65 6d 70 74 3d 4c 6f 67   LoginAtt empt=Log
0070   2b 69 6e 26 77 70 4c 6f  67 69 6e 54 6f 6b 65 6e   +in&wpLo ginToken
0080   3d 35 38 38 37 36 32 66  32 38 66 33 33 61 66 34   =588762f 28f33af4
0090   66 61 39 39 34 64 63 65  62 64 37 66 64 30 38 65   fa994dce bd7fd08e
00a0   34                                                 4
```

```
Data (data.data), 107 bytes    Packets: 33 Displayed: 33 Marked: 0 Dropped: 0
```


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

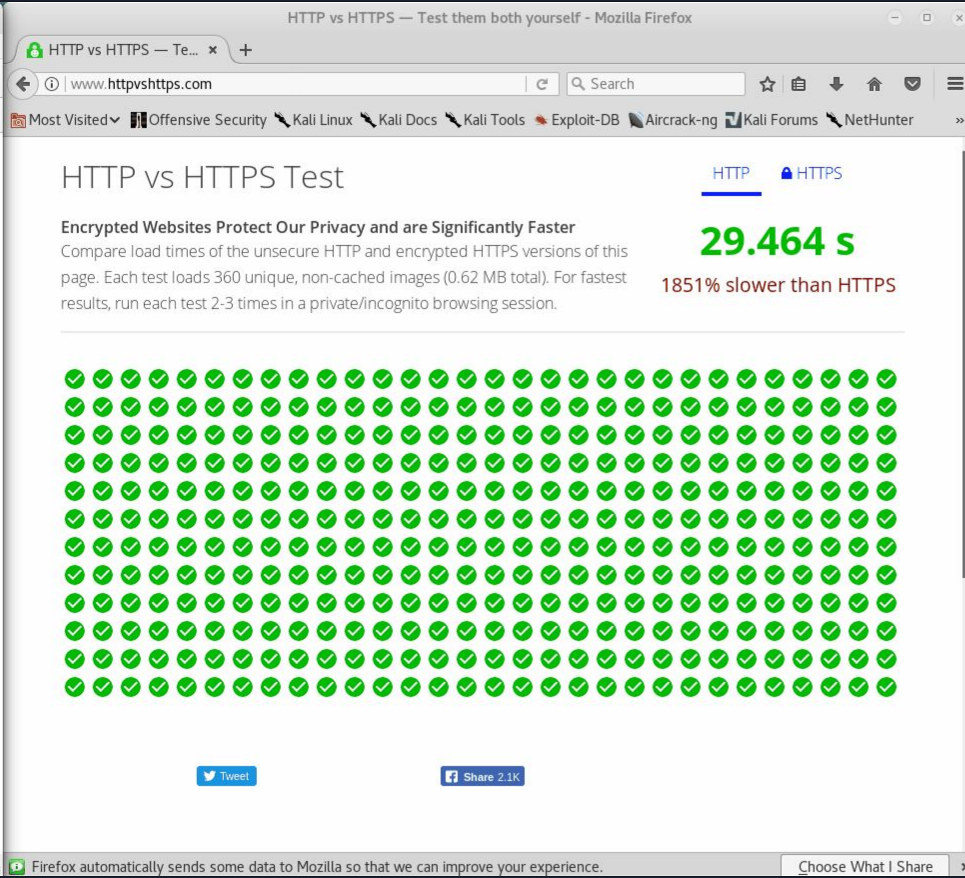
```
eth0
any
Loopback: lo
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: ciscodump
Random packet generator: randpkt
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

Ready to load or capture | No Packets | Profile: Default



HTTP vs HTTPS Test

Encrypted Websites Protect Our Privacy and are Significantly Faster

Compare load times of the unsecure HTTP and encrypted HTTPS versions of this page. Each test loads 360 unique, non-cached images (0.62 MB total). For fastest results, run each test 2-3 times in a private/incognito browsing session.

29.464 s

1851% slower than HTTPS

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

CTF - Forensics

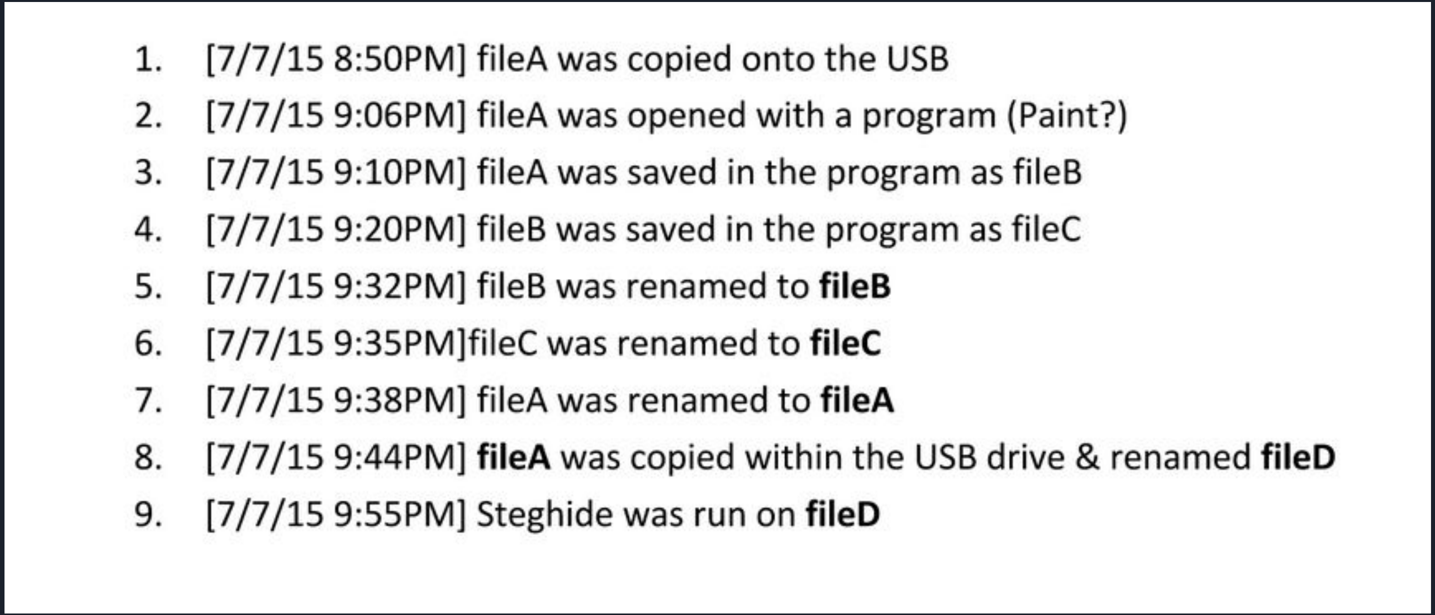
- General CTF challenges for forensics
  - File Formats
  - Metadata (EXIF data)
  - Steganography

CTF - File Formats

- **File Signatures** are bytes within a file used to identify the format of the file (2-4 bytes long, found at beginning of file)
- Bytes:
  - FFD8FFE0 00104A46 494600
- Ascii:
  - ˇÿˇ‡ JFIF

CTF - Metadata

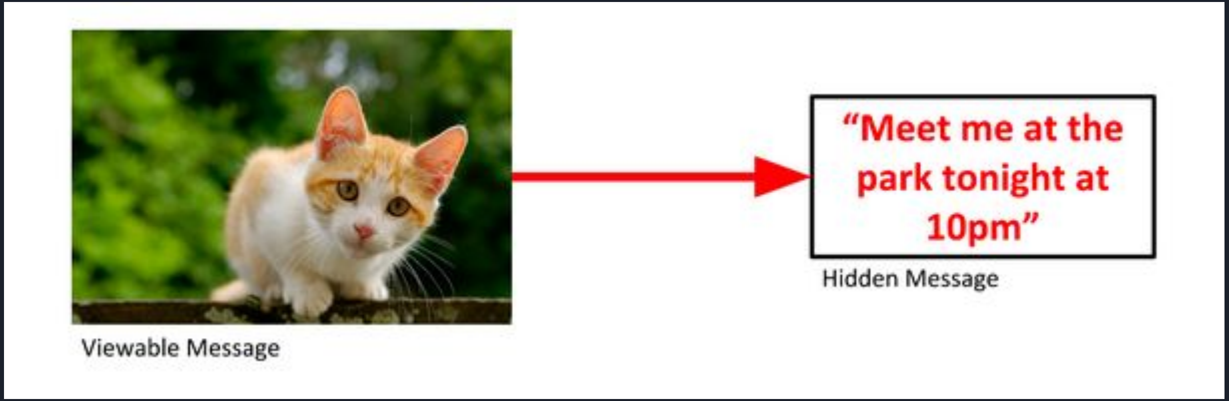
- Metadata is data about data.
  - Dates, camera info, GPS, **Timestamps**, etc.
- Tools: exiftool



1. [7/7/15 8:50PM] fileA was copied onto the USB
2. [7/7/15 9:06PM] fileA was opened with a program (Paint?)
3. [7/7/15 9:10PM] fileA was saved in the program as fileB
4. [7/7/15 9:20PM] fileB was saved in the program as fileC
5. [7/7/15 9:32PM] fileB was renamed to **fileB**
6. [7/7/15 9:35PM]fileC was renamed to **fileC**
7. [7/7/15 9:38PM] fileA was renamed to **fileA**
8. [7/7/15 9:44PM] **fileA** was copied within the USB drive & renamed **fileD**
9. [7/7/15 9:55PM] Steghide was run on **fileD**

CTF - Steganography

- Steganography is the practice of hiding data in plain sight.
- Steganography is often embedded in images or audio.
- Tools: binwalk, stegoVeritas, Stegsolve



Steganography Demo

File #1: http://tiny.cc/z2oifz
File #2: http://tiny.cc/41oifz

NOVEMBER 1 – 2

TexSAW

2019

9th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING AND COMPUTER SCIENCE