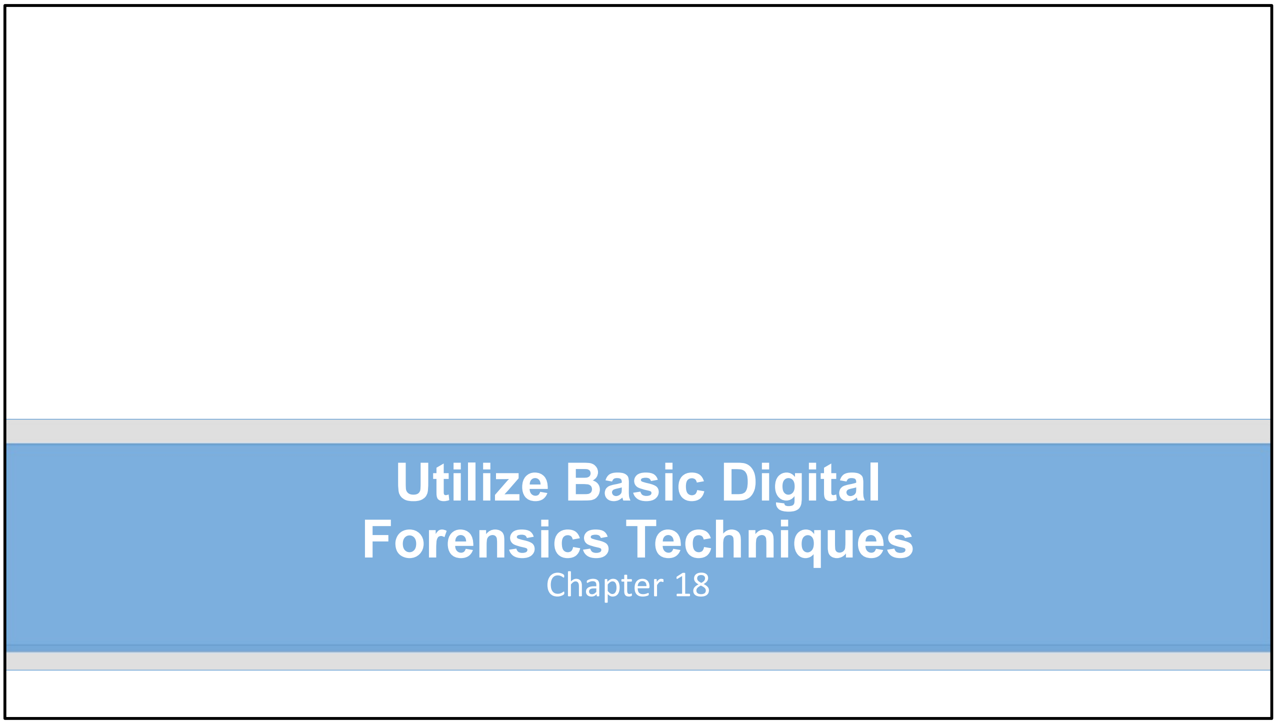


Utilize Basic Digital Forensics Techniques

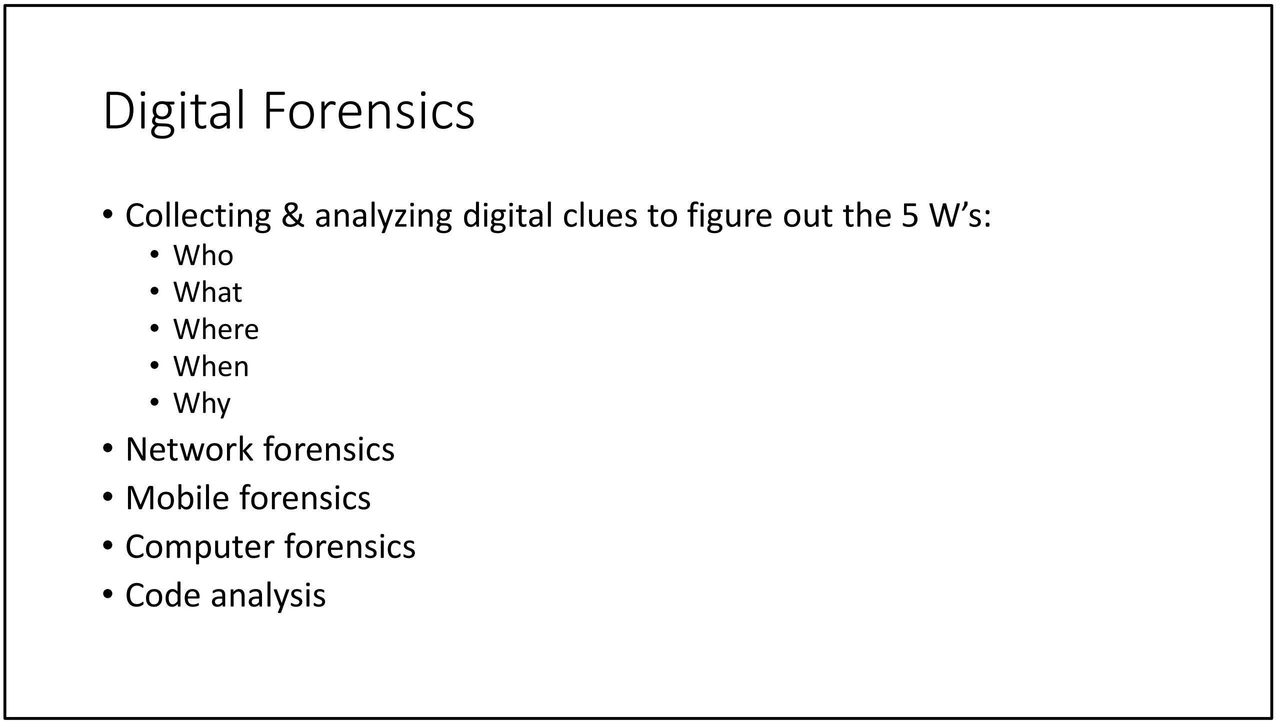
Chapter 18

Episode 18.01

Digital Forensics

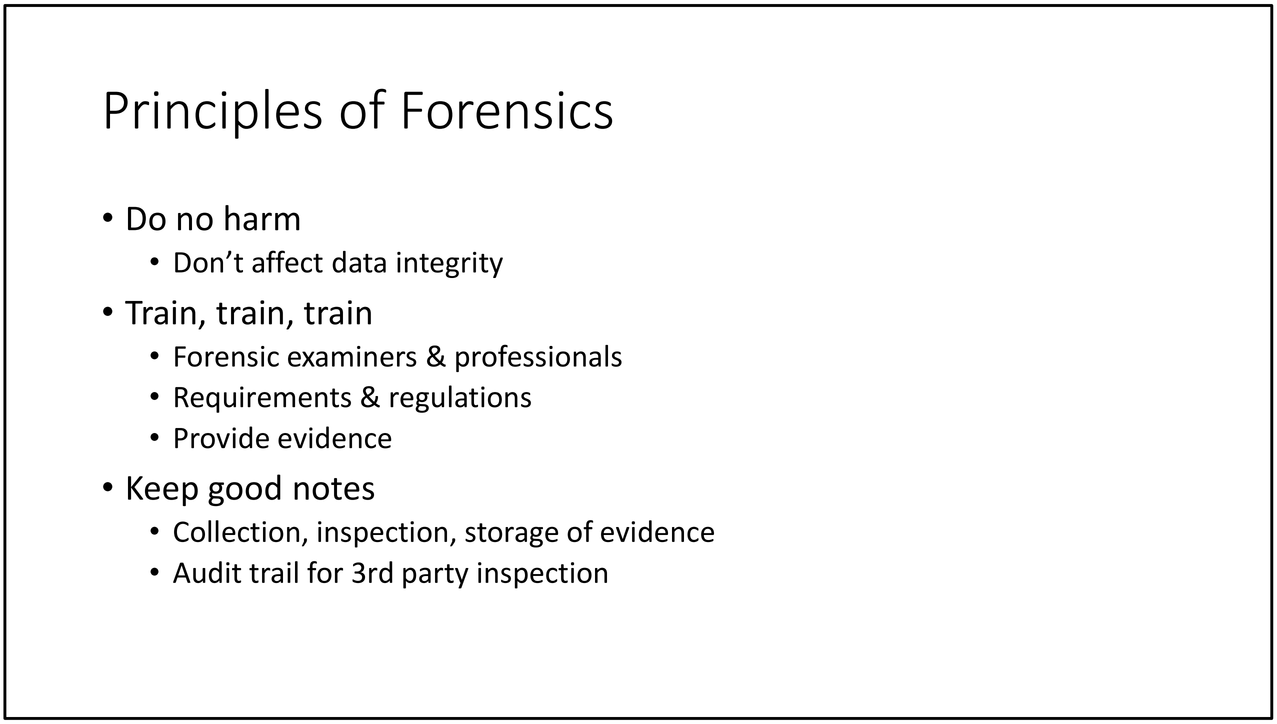
Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.

- Procedures
- Data acquisition
- Legal hold



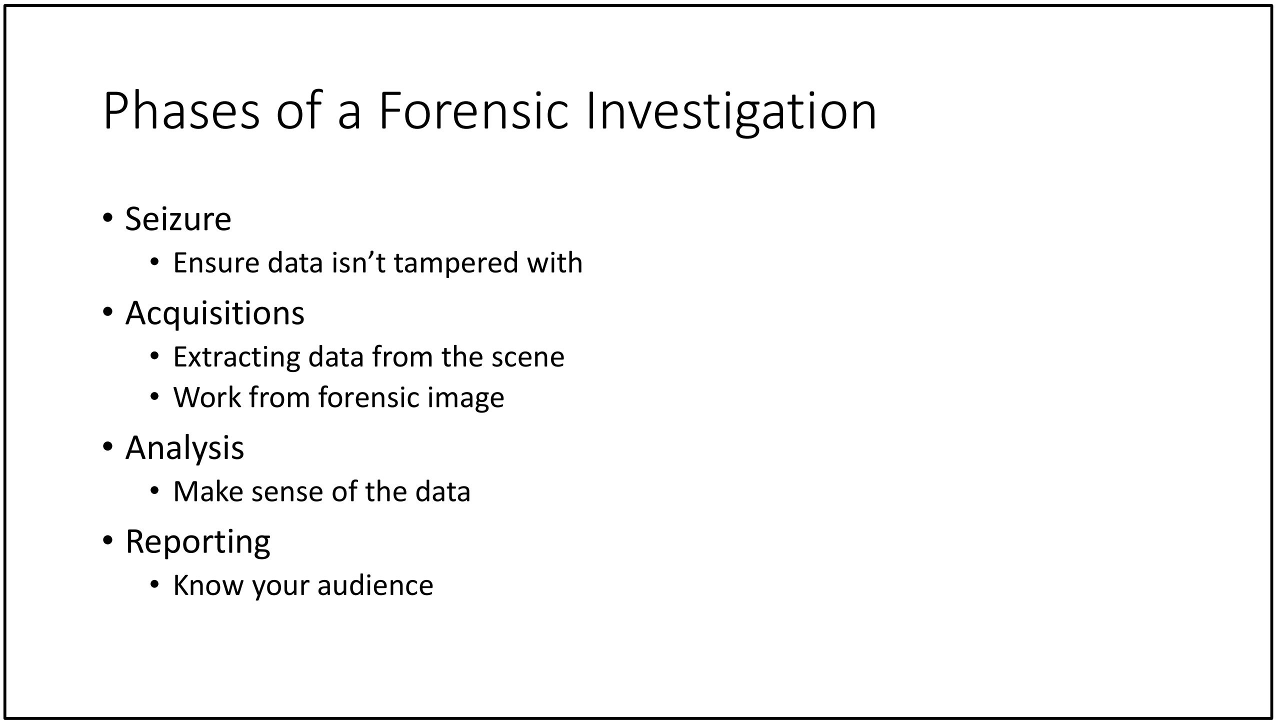
Digital Forensics

- Collecting & analyzing digital clues to figure out the 5 W’s:
  - Who
  - What
  - Where
  - When
  - Why
- Network forensics
- Mobile forensics
- Computer forensics
- Code analysis



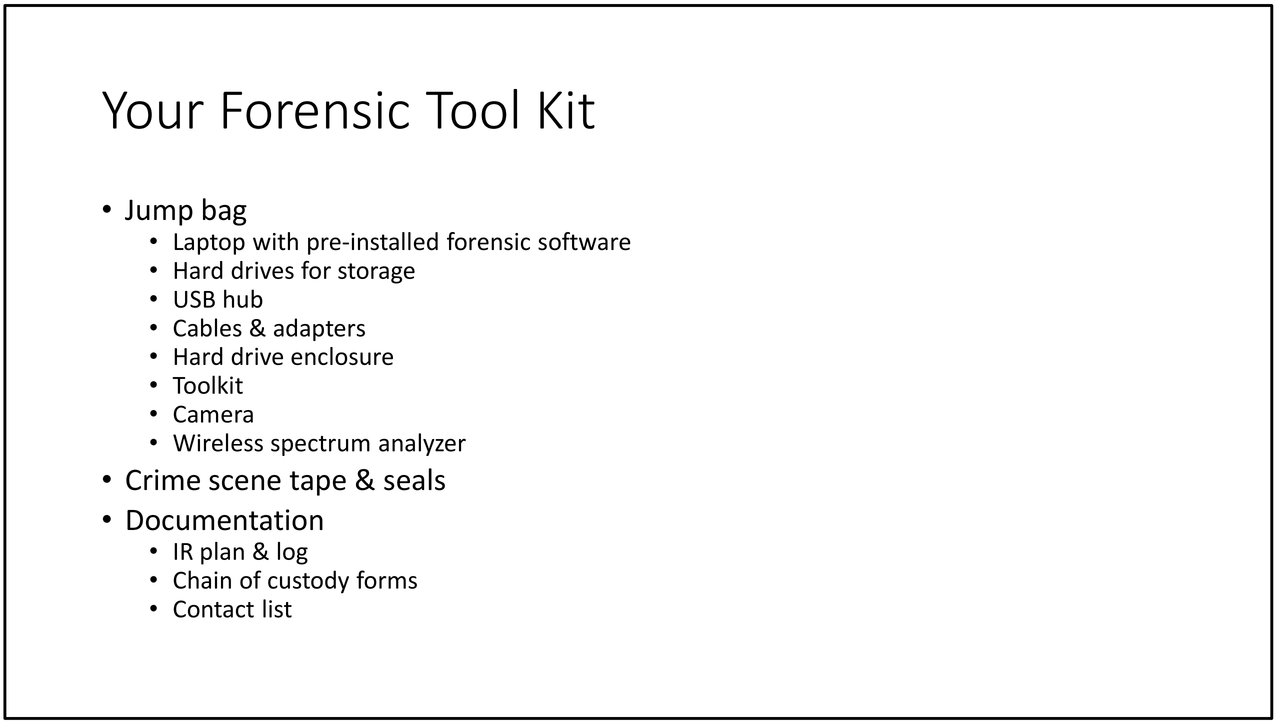
Principles of Forensics

- Do no harm
  - Don’t affect data integrity
- Train, train, train
  - Forensic examiners & professionals
  - Requirements & regulations
  - Provide evidence
- Keep good notes
  - Collection, inspection, storage of evidence
  - Audit trail for 3rd party inspection



Phases of a Forensic Investigation

- Seizure
  - Ensure data isn’t tampered with
- Acquisitions
  - Extracting data from the scene
  - Work from forensic image
- Analysis
  - Make sense of the data
- Reporting
  - Know your audience



Your Forensic Tool Kit

- Jump bag
  - Laptop with pre-installed forensic software
  - Hard drives for storage
  - USB hub
  - Cables & adapters
  - Hard drive enclosure
  - Toolkit
  - Camera
  - Wireless spectrum analyzer
- Crime scene tape & seals
- Documentation
  - IR plan & log
  - Chain of custody forms
  - Contact list

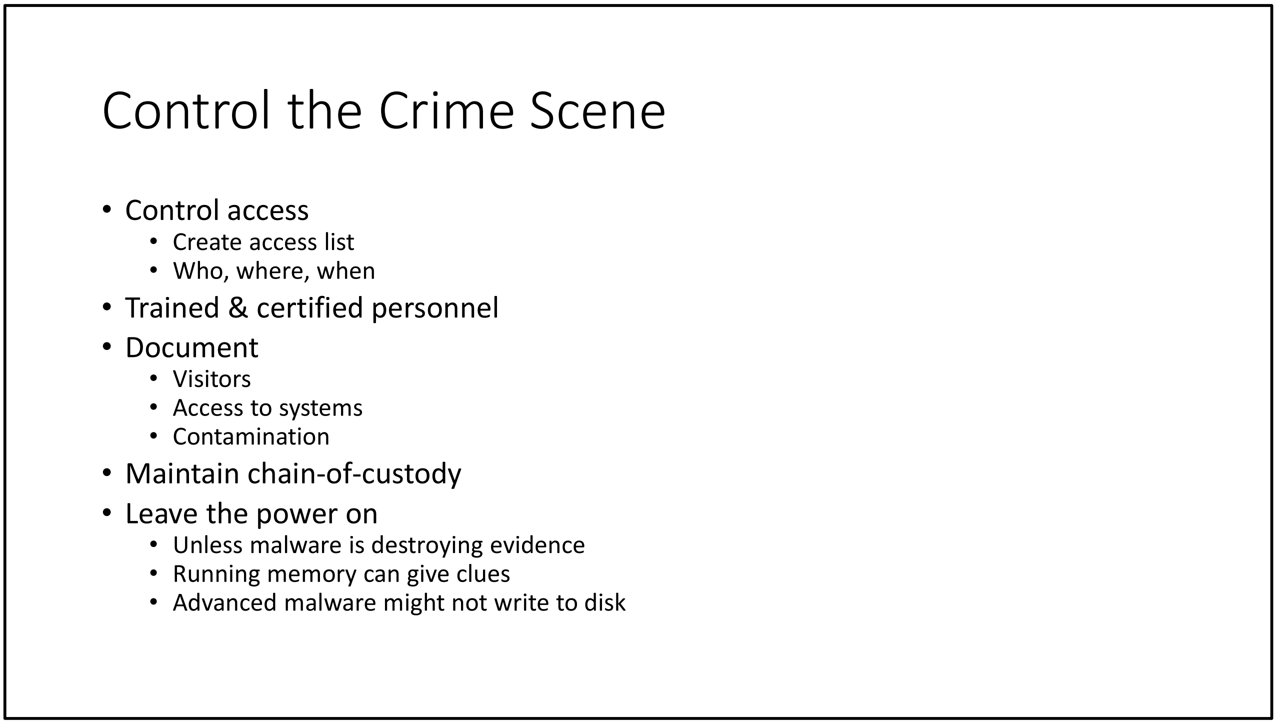
Episode 18.02

Seizure & Acquisitions

Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.

• Endpoint

- Disk
- Memory

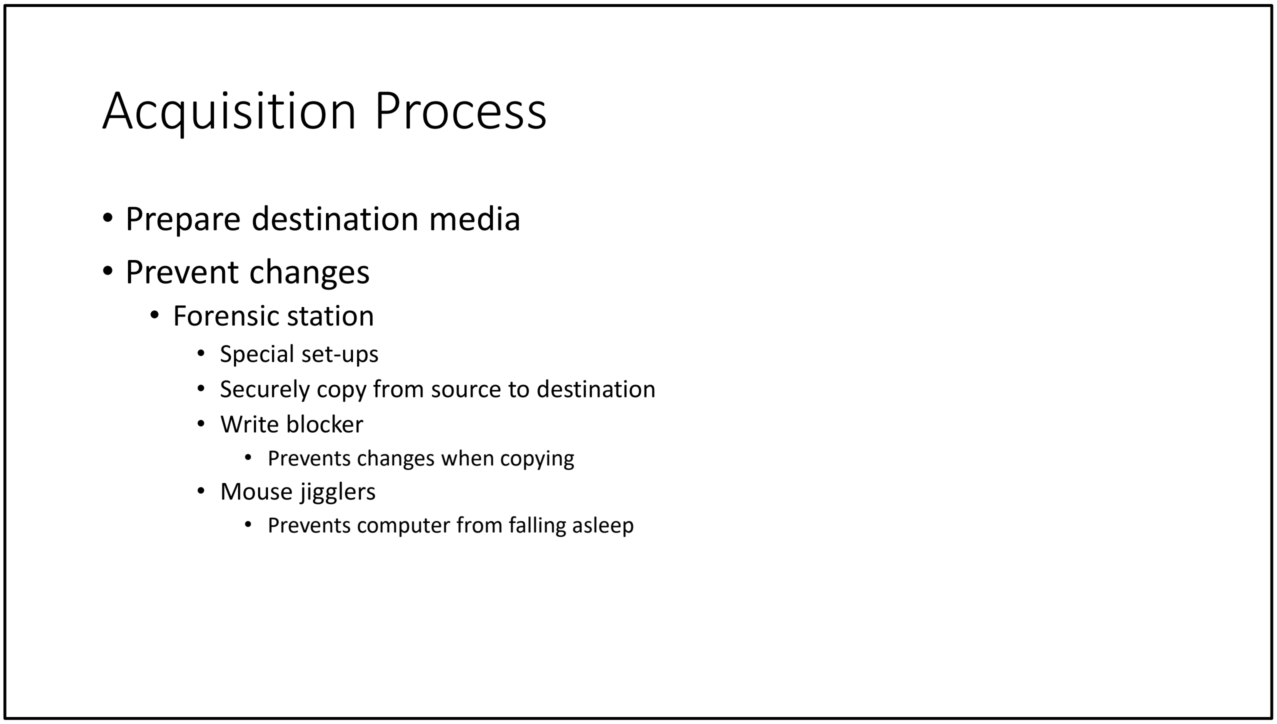


Control the Crime Scene

- Control access
  - Create access list
  - Who, where, when
- Trained & certified personnel
- Document
  - Visitors
  - Access to systems
  - Contamination
- Maintain chain-of-custody
- Leave the power on
  - Unless malware is destroying evidence
  - Running memory can give clues
  - Advanced malware might not write to disk

Acquisition Process

- Prepare destination media
  - Securely store data
  - Removable hard drive or network-based option
  - Make sure destination media is clean



Acquisition Process

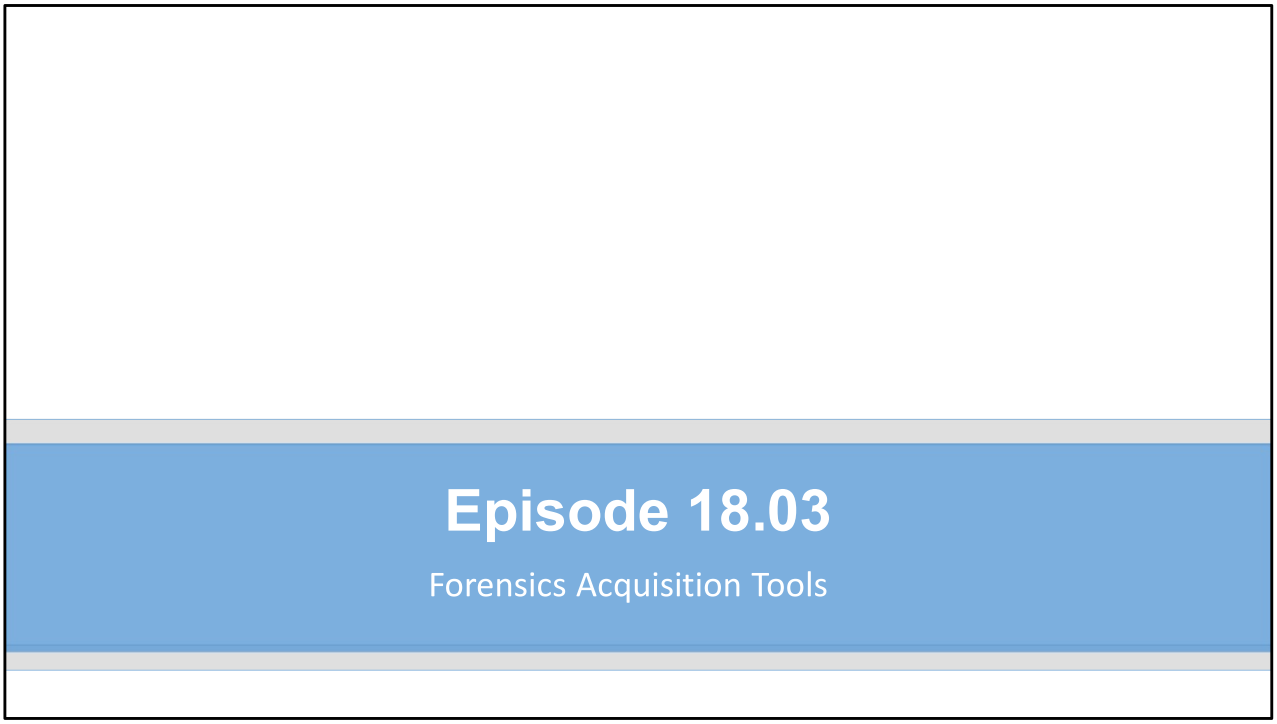
- Prepare destination media
- Prevent changes
  - Forensic station
    - Special set-ups
    - Securely copy from source to destination
    - Write blocker
      - Prevents changes when copying
    - Mouse jigglers
      - Prevents computer from falling asleep

Forensics Station

https://www.cru-inc.com/product_image_galleries/Forensic_Field_Kit_D/5-Ditto_Field_Kit.jpg

Write Blocker

https://www.cru-inc.com/wp-content/uploads/2016/05/DittoDX_angle1-3.png



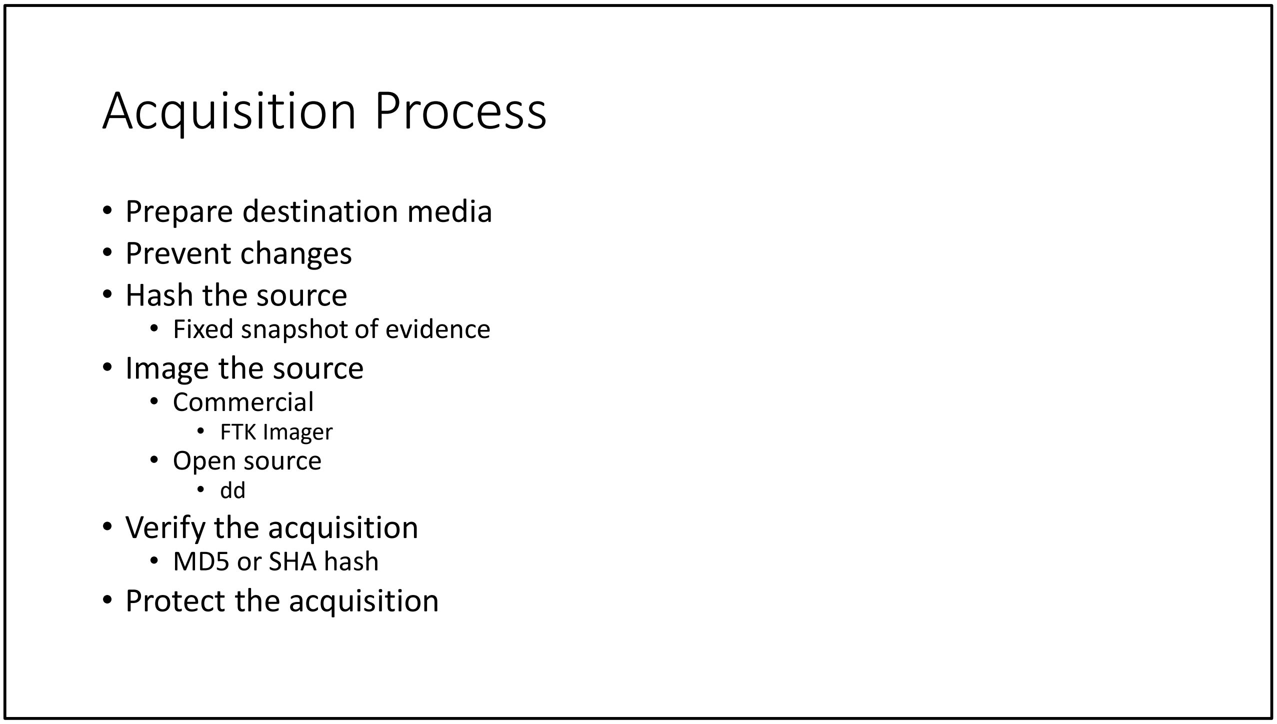
Episode 18.03

Forensics Acquisition Tools

Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.

• Hashing

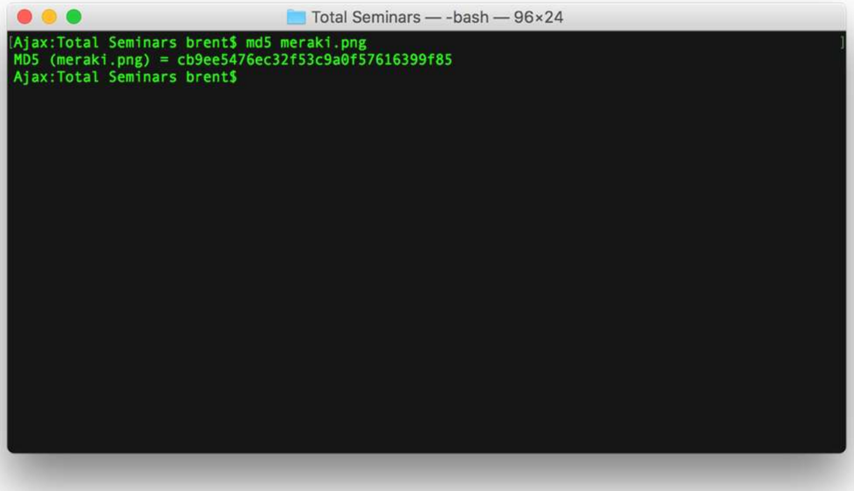
- Changes to binaries



Acquisition Process

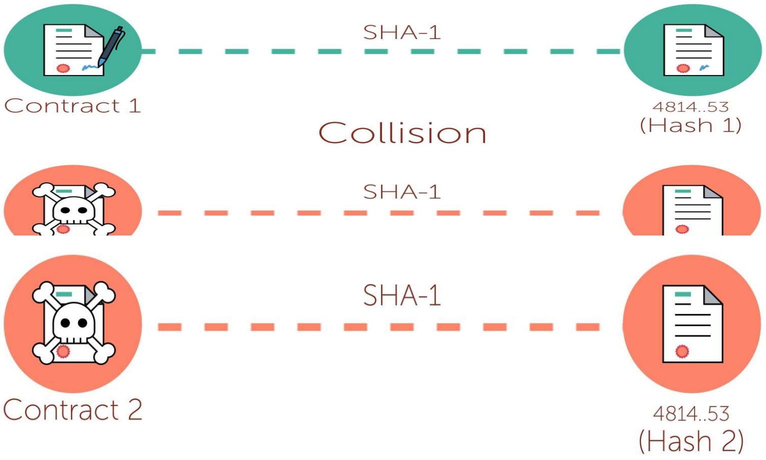
- Prepare destination media
- Prevent changes
- Hash the source
  - Fixed snapshot of evidence
- Image the source
  - Commercial
    - FTK Imager
  - Open source
    - dd
- Verify the acquisition
  - MD5 or SHA hash
- Protect the acquisition

Hash Demo

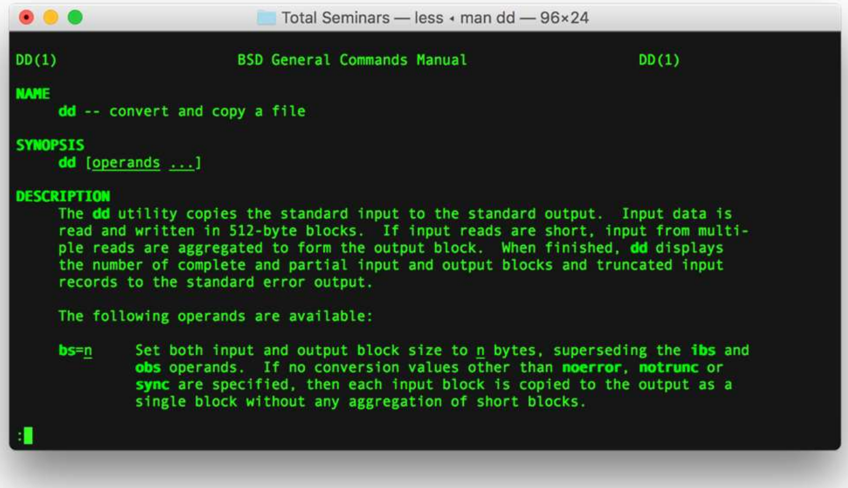


```
Ajax:Total Seminars brent$ md5 meraki.png
MD5 (meraki.png) = cb9ee5476ec32f53c9a0f57616399f85
Ajax:Total Seminars brent$
```

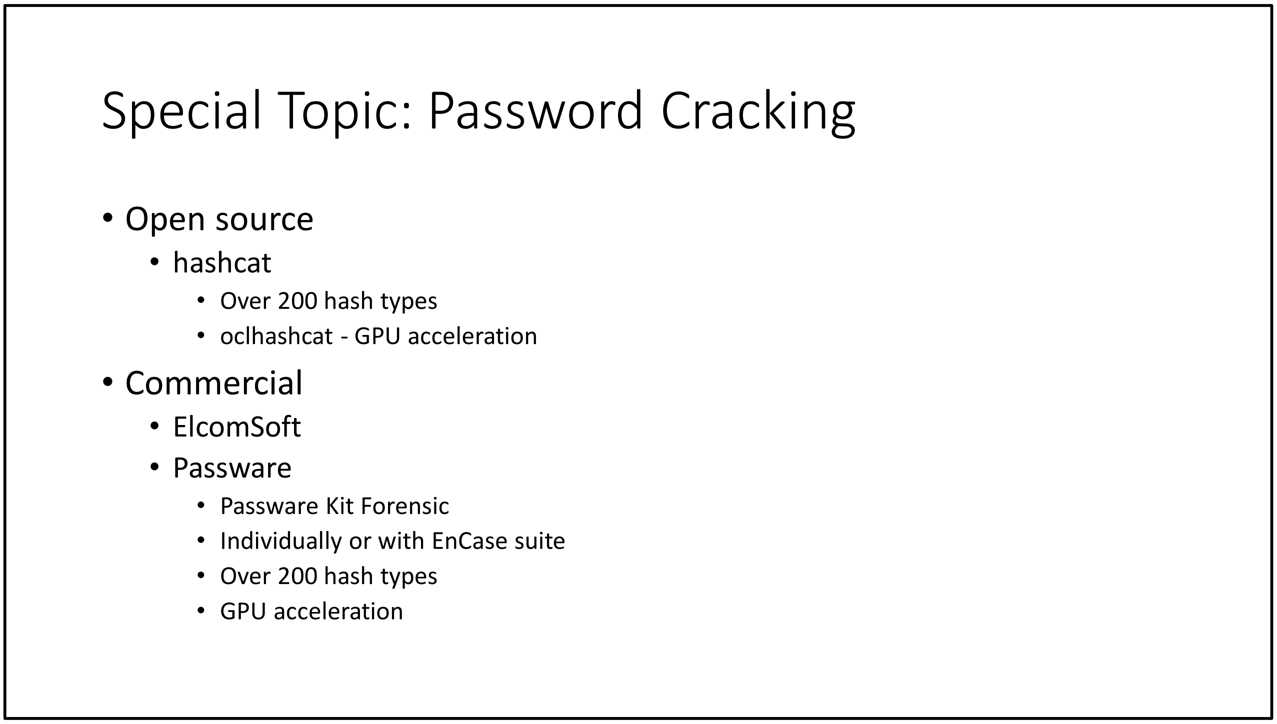
Hash Collisions



dd Demo

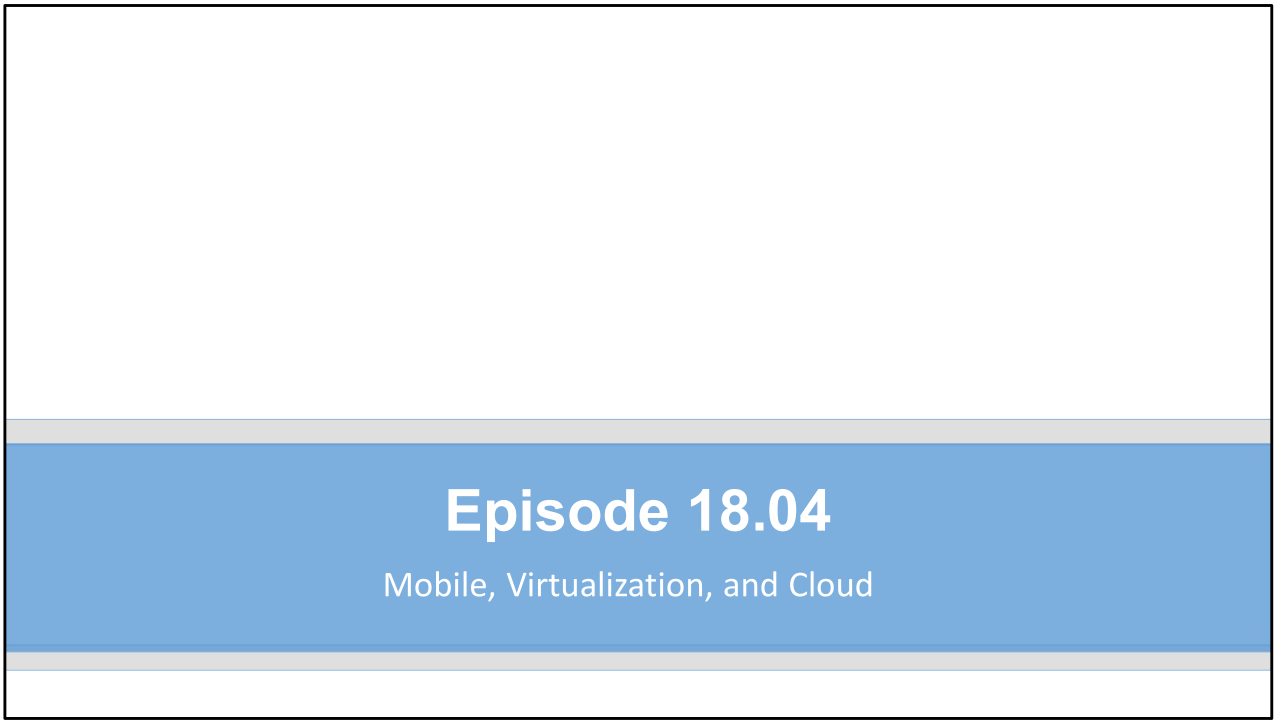


```
DD(1)                     BSD General Commands Manual                    DD(1)

NAME
     dd -- convert and copy a file

SYNOPSIS
     dd [operands ...]

DESCRIPTION
     The dd utility copies the standard input to the standard output.  Input data is
     read and written in 512-byte blocks.  If input reads are short, input from multi-
     ple reads are aggregated to form the output block.  When finished, dd displays
     the number of complete and partial input and output blocks and truncated input
     records to the standard error output.

     The following operands are available:

     bs=n     Set both input and output block size to n bytes, superseding the ibs and
              obs operands.  If no conversion values other than noerror, notrunc or
              sync are specified, then each input block is copied to the output as a
              single block without any aggregation of short blocks.

:
```



Special Topic: Password Cracking

- Open source
  - hashcat
    - Over 200 hash types
    - oclhashcat - GPU acceleration
- Commercial
  - ElcomSoft
  - Passware
    - Passware Kit Forensic
    - Individually or with EnCase suite
    - Over 200 hash types
    - GPU acceleration

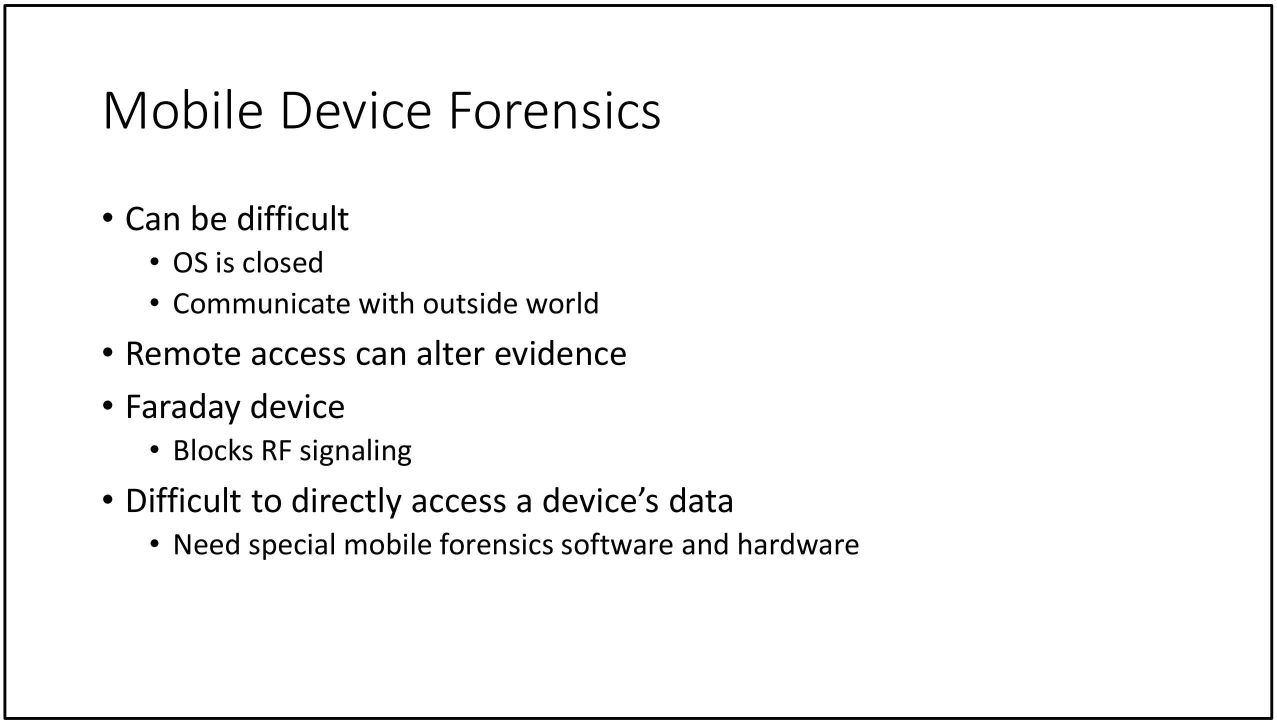


Episode 18.04

Mobile, Virtualization, and Cloud

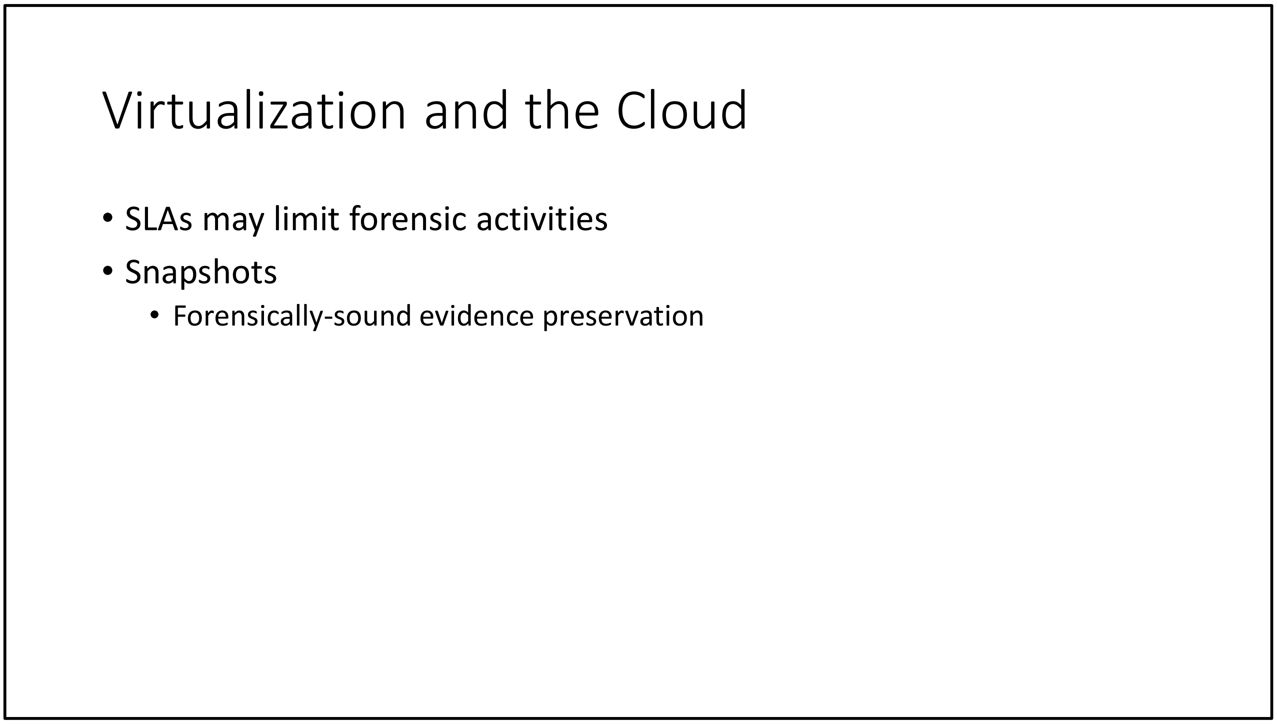
Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.

- Mobile
- Cloud
- Virtualization



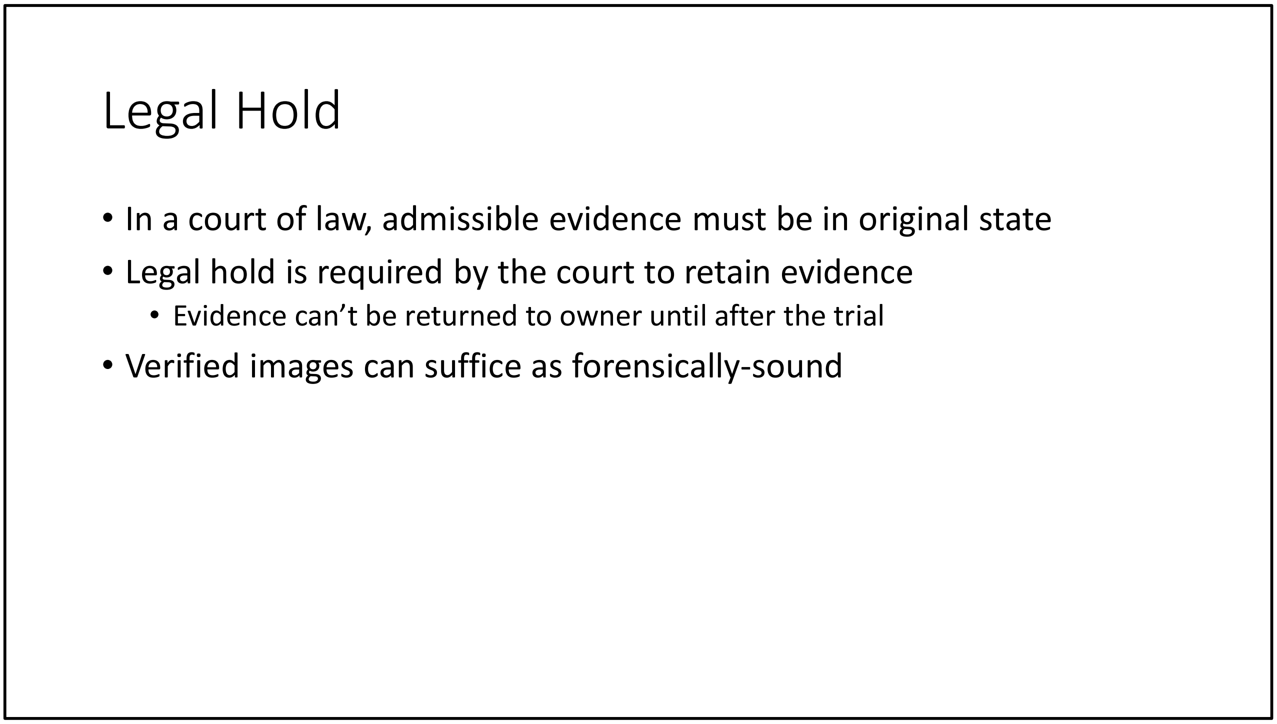
Mobile Device Forensics

- Can be difficult
  - OS is closed
  - Communicate with outside world
- Remote access can alter evidence
- Faraday device
  - Blocks RF signaling
- Difficult to directly access a device’s data
  - Need special mobile forensics software and hardware



Virtualization and the Cloud

- SLAs may limit forensic activities
- Snapshots
  - Forensically-sound evidence preservation



Legal Hold

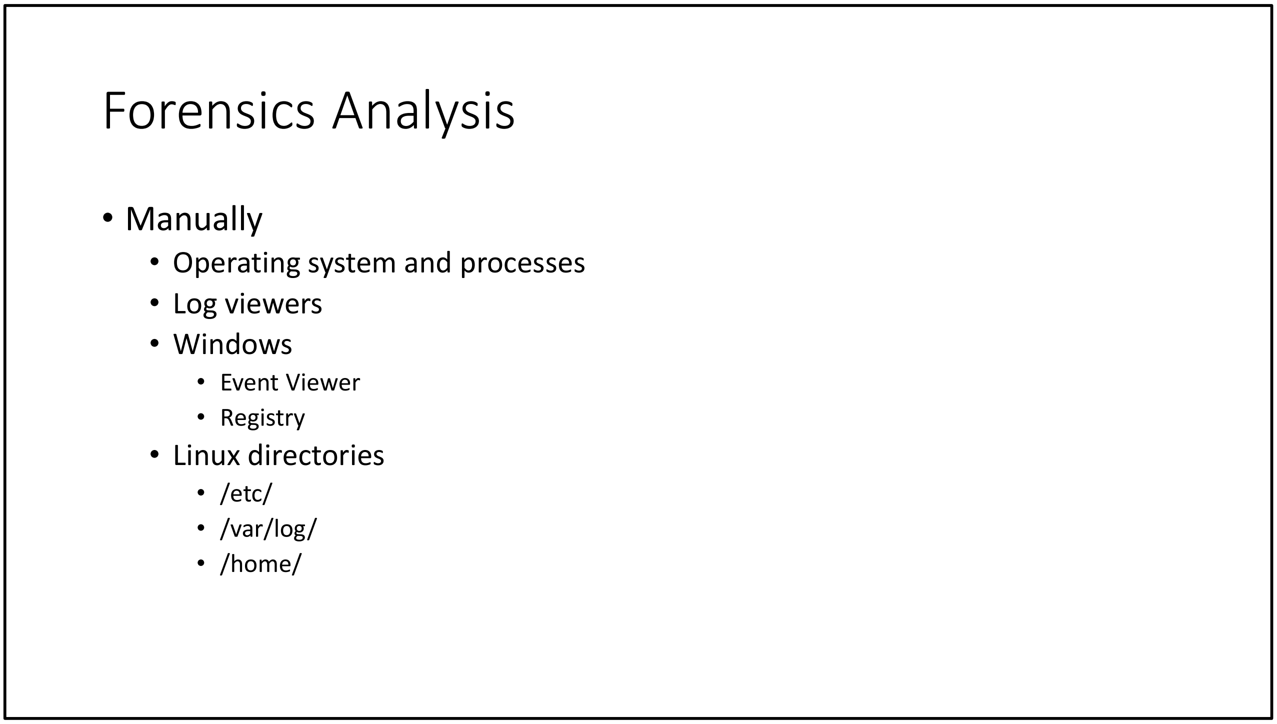
- In a court of law, admissible evidence must be in original state
- Legal hold is required by the court to retain evidence
  - Evidence can’t be returned to owner until after the trial
- Verified images can suffice as forensically-sound

Episode 18.05

Forensics Analysis: Part 1

Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.

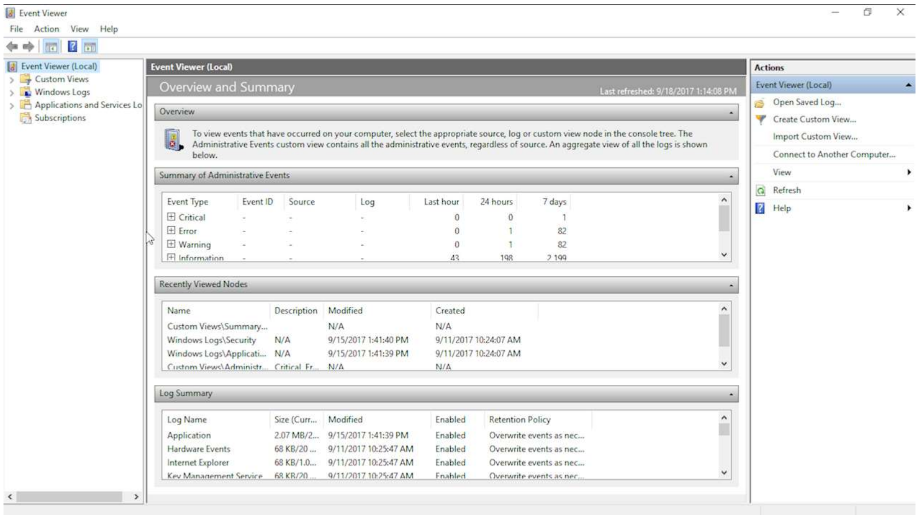
- Procedures



Forensics Analysis

- Manually
  - Operating system and processes
  - Log viewers
  - Windows
    - Event Viewer
    - Registry
  - Linux directories
    - /etc/
    - /var/log/
    - /home/

Windows Utilities Demo



Event Viewer (Local)

Overview and Summary

Last refreshed: 9/18/2017 1:14:08 PM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
⊞ Critical	-	-	-	0	0	1
⊞ Error	-	-	-	0	1	82
⊞ Warning	-	-	-	0	1	82
⊞ Information	-	-	-	43	198	2 199

Recently Viewed Nodes

Name	Description	Modified	Created
Custom Views\Summary...		N/A	N/A
Windows Logs\Security	N/A	9/15/2017 1:41:40 PM	9/11/2017 10:24:07 AM
Windows Logs\Applicati...	N/A	9/15/2017 1:41:39 PM	9/11/2017 10:24:07 AM
Custom Views\Administr...	Critical, Er...	N/A	N/A

Log Summary

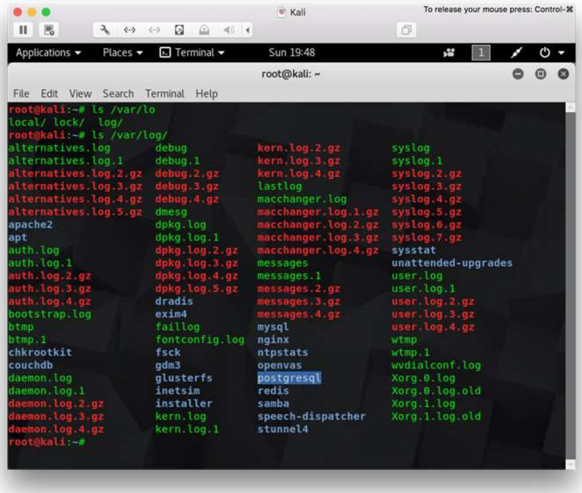
Log Name	Size (Curr...	Modified	Enabled	Retention Policy
Application	2.07 MB/2...	9/15/2017 1:41:39 PM	Enabled	Overwrite events as nec...
Hardware Events	68 KB/20 ...	9/11/2017 10:25:47 AM	Enabled	Overwrite events as nec...
Internet Explorer	68 KB/1.0...	9/11/2017 10:25:47 AM	Enabled	Overwrite events as nec...
Key Management Service	68 KB/20 ...	9/11/2017 10:25:47 AM	Enabled	Overwrite events as nec...

Episode 18.06

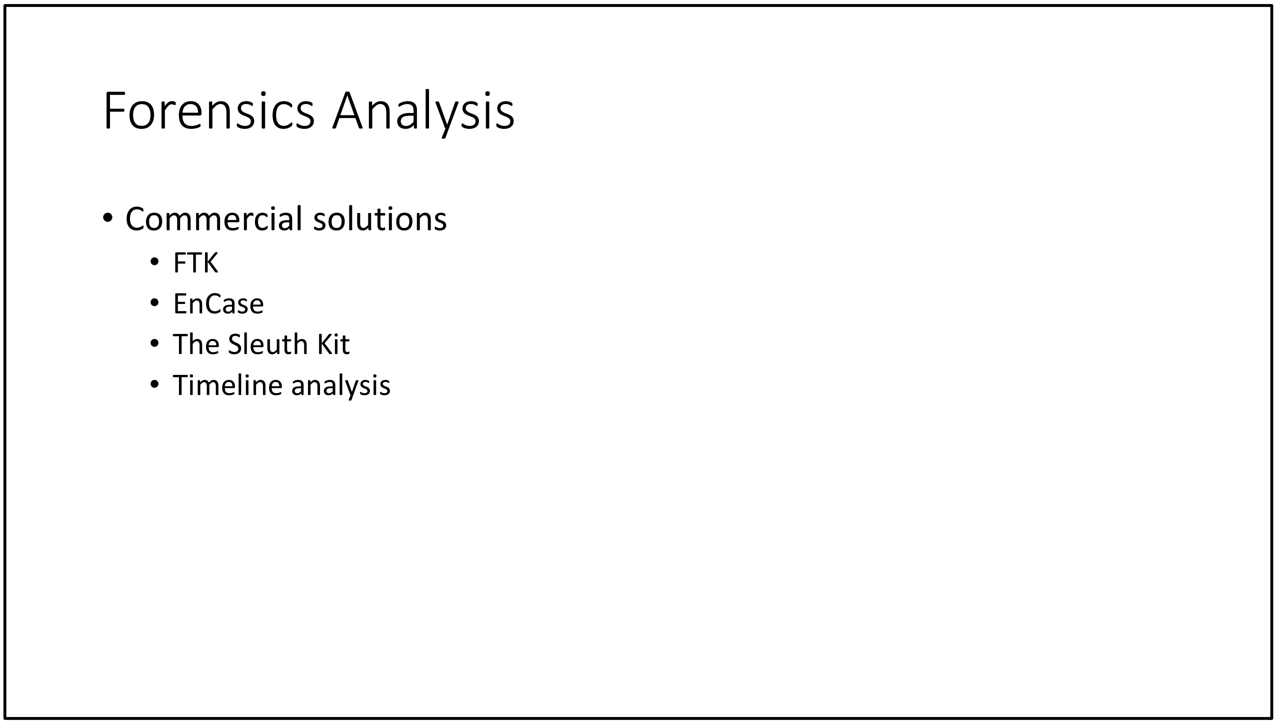
Forensics Analysis: Part 2

Objective: 4.4 Given a scenario, utilize basic digital forensics techniques.
- Procedures

Linux Forensics Demo

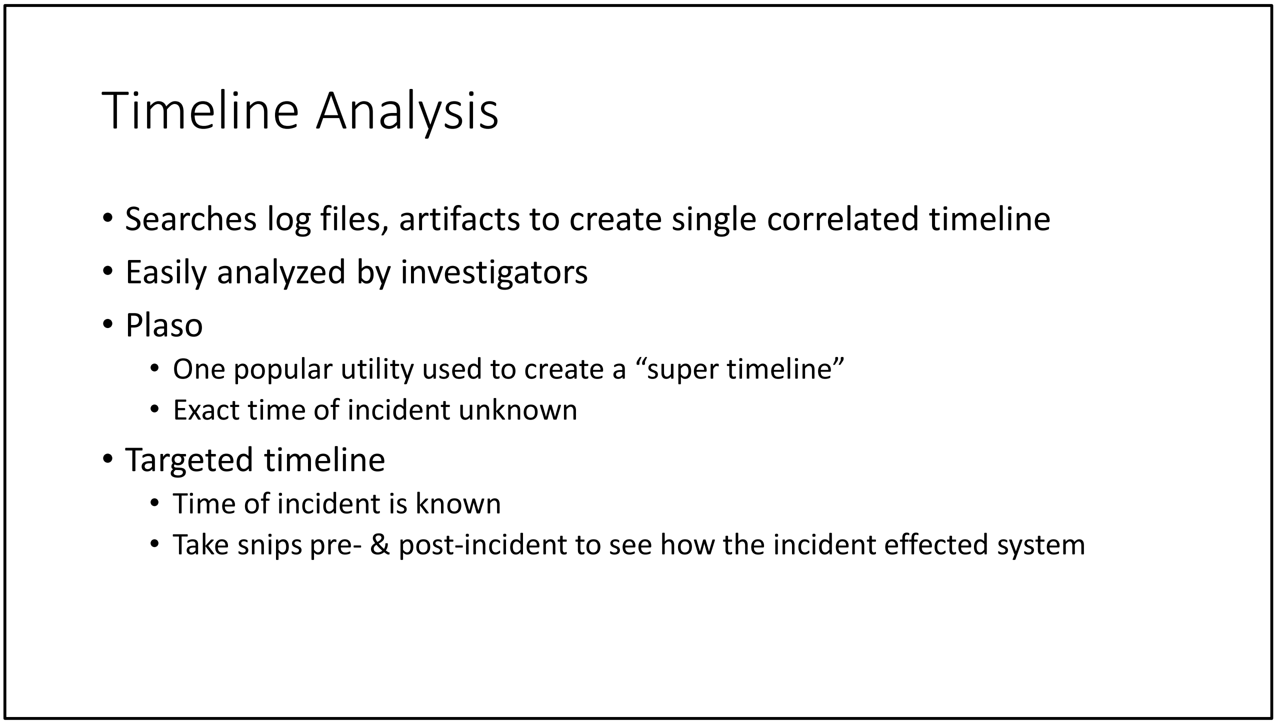


```
root@kali:~# ls /var/lo
local/ lock/  log/
root@kali:~# ls /var/log/
alternatives.log       debug           kern.log.2.gz        syslog
alternatives.log.1     debug.1         kern.log.3.gz        syslog.1
alternatives.log.2.gz  debug.2.gz      kern.log.4.gz        syslog.2.gz
alternatives.log.3.gz  debug.3.gz      lastlog              syslog.3.gz
alternatives.log.4.gz  debug.4.gz      macchanger.log       syslog.4.gz
alternatives.log.5.gz  dmesg           macchanger.log.1.gz  syslog.5.gz
apache2                dpkg.log        macchanger.log.2.gz  syslog.6.gz
apt                    dpkg.log.1      macchanger.log.3.gz  syslog.7.gz
auth.log               dpkg.log.2.gz   macchanger.log.4.gz  sysstat
auth.log.1             dpkg.log.3.gz   messages             unattended-upgrades
auth.log.2.gz          dpkg.log.4.gz   messages.1           user.log
auth.log.3.gz          dpkg.log.5.gz   messages.2.gz        user.log.1
auth.log.4.gz          dradis          messages.3.gz        user.log.2.gz
bootstrap.log          exim4           messages.4.gz        user.log.3.gz
btmp                   faillog         mysql                user.log.4.gz
btmp.1                 fontconfig.log  nginx                wtmp
chkrootkit             fsck            ntpstats             wtmp.1
couchdb                gdm3            openvas              wvdialconf.log
daemon.log             glusterfs       postgresql           Xorg.0.log
daemon.log.1           inetsim         redis                Xorg.0.log.old
daemon.log.2.gz        installer       samba                Xorg.1.log
daemon.log.3.gz        kern.log        speech-dispatcher    Xorg.1.log.old
daemon.log.4.gz        kern.log.1      stunnel4
root@kali:~#
```



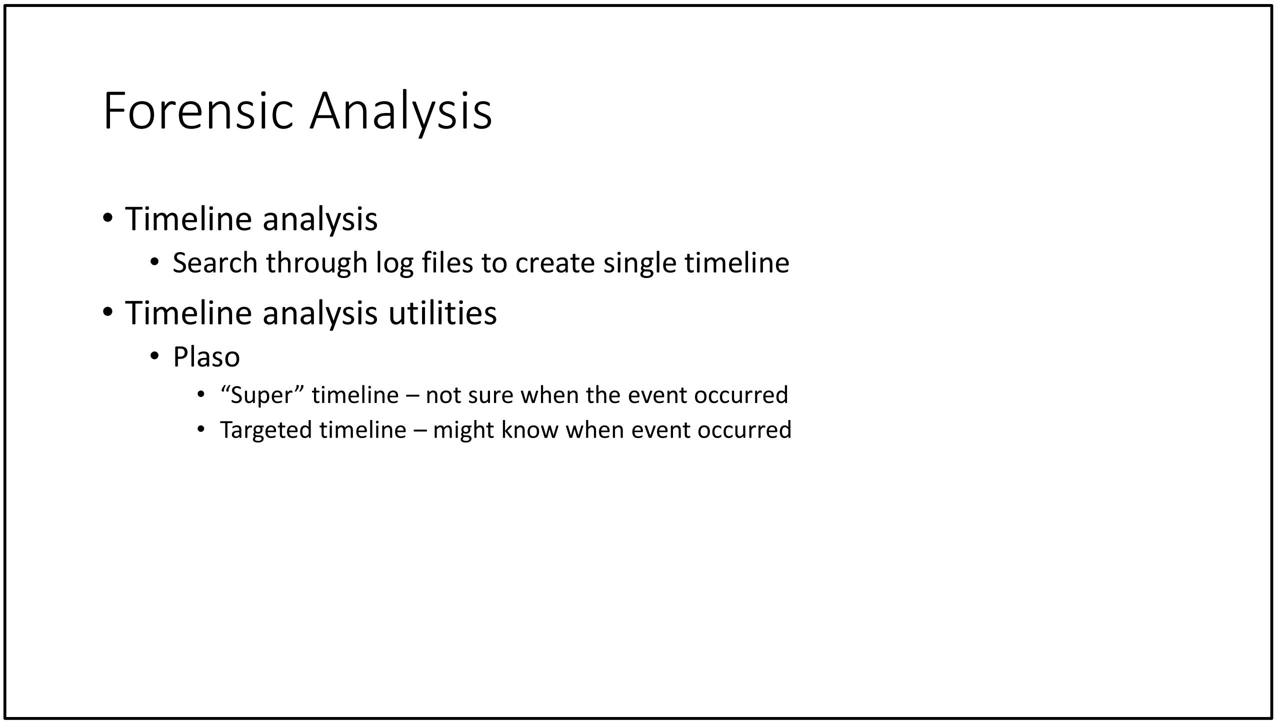
Forensics Analysis

- Commercial solutions
  - FTK
  - EnCase
  - The Sleuth Kit
  - Timeline analysis



Timeline Analysis

- Searches log files, artifacts to create single correlated timeline
- Easily analyzed by investigators
- Plaso
  - One popular utility used to create a “super timeline”
  - Exact time of incident unknown
- Targeted timeline
  - Time of incident is known
  - Take snips pre- & post-incident to see how the incident effected system



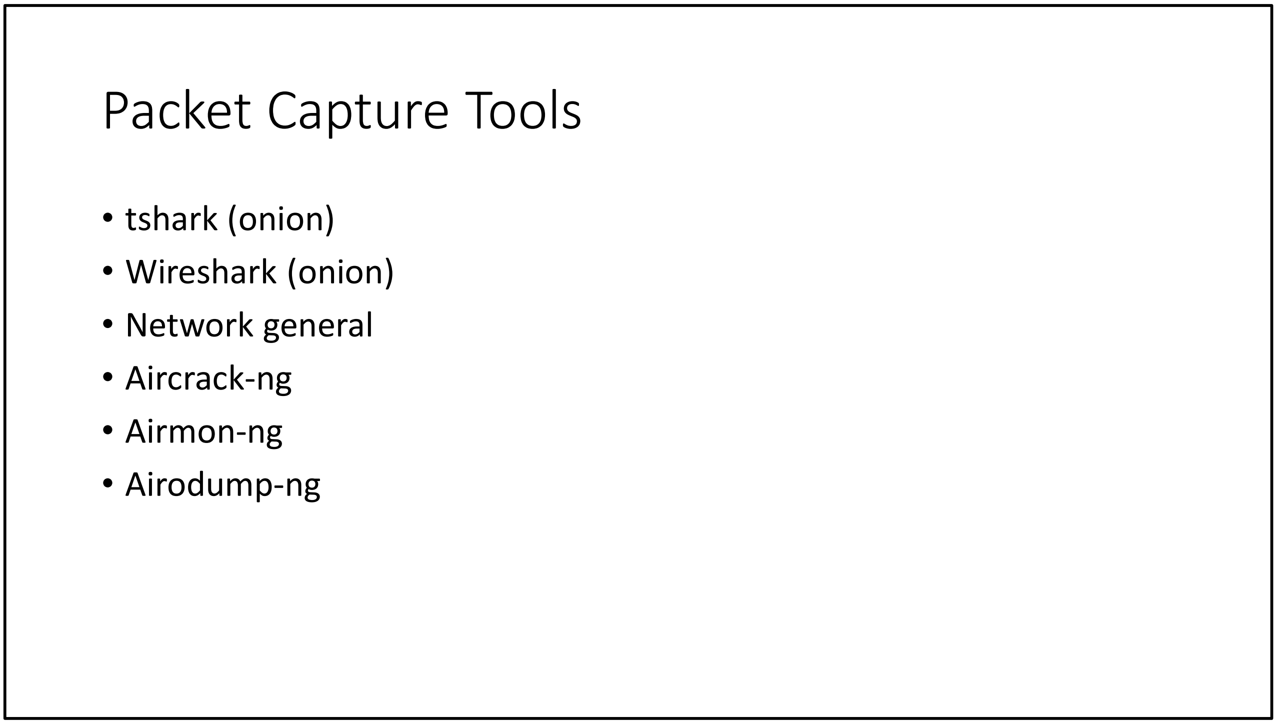
Forensic Analysis

- Timeline analysis
  - Search through log files to create single timeline
- Timeline analysis utilities
  - Plaso
    - “Super” timeline – not sure when the event occurred
    - Targeted timeline – might know when event occurred

Episode 18.07

Packet Capture

• Network
- Wireshark



Packet Capture Tools

- tshark (onion)
- Wireshark (onion)
- Network general
- Aircrack-ng
- Airmon-ng
- Airodump-ng