2019
SAN FRANCISCO
BSIDES

IMPLEMENTING A KICK-BUTT TRAINING PROGRAM: BLUE TEAM GO!

Ryan J. Chapman
@rj_chap

AGENDA

- Why baseline training?
- Trainers
- **Core Tenants**
- Delivery Methodologies
- The curriculum!
  - **Five different phases**
- Reinforcement
- Questions / Wrap-up

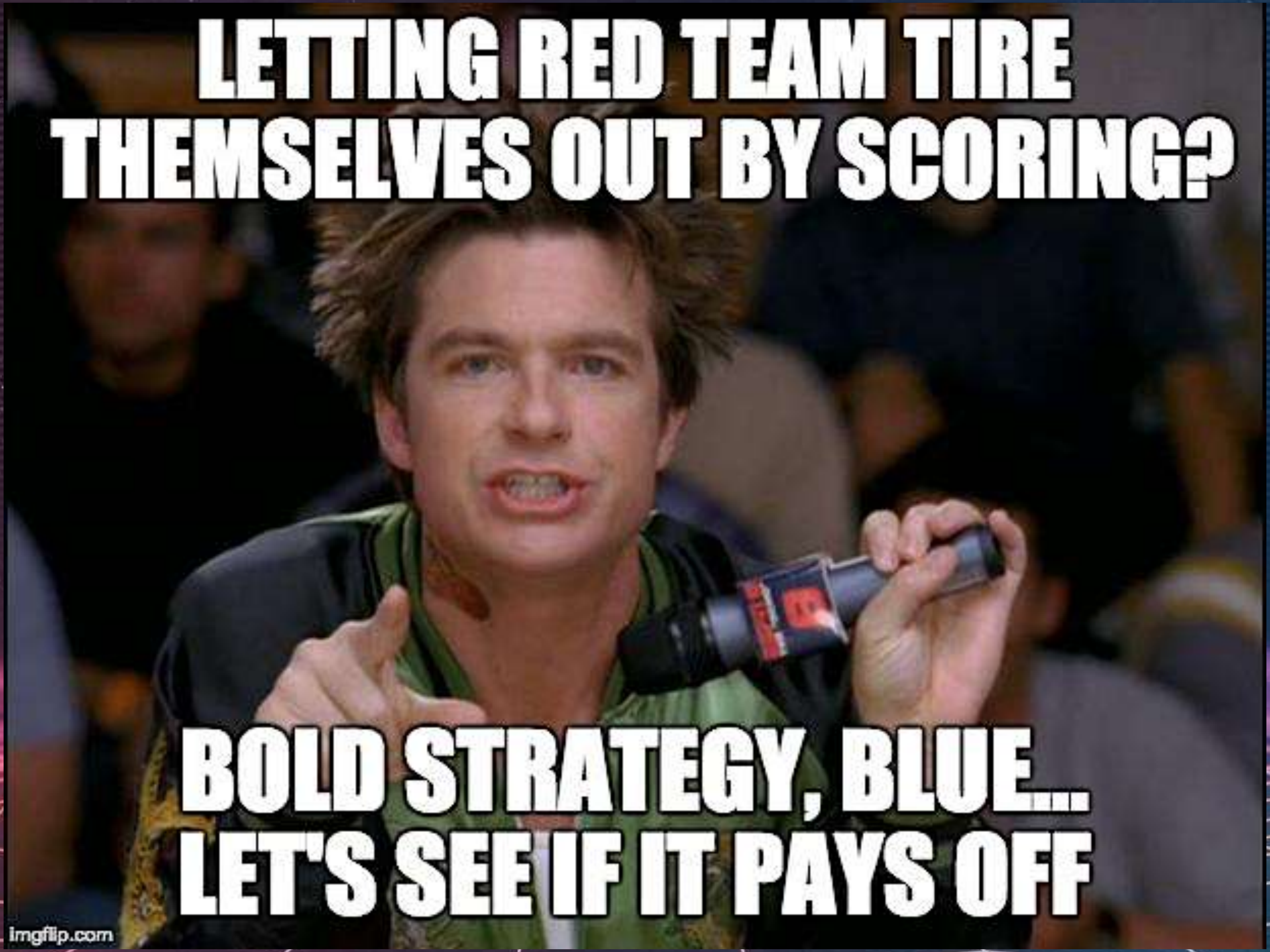
ABOUT ME – @RJ_CHAP

I LOVE THE POWER GLOVE…
IT'S SO BAD

WHY BASELINE TRAINING?

(Wittmeyer, n.d.)

- Finding the “right” hire
- Failure analysis:
  - Educational institutions
  - Certifications
  - Hiring “the analyst mindset”
  - Previous experience


LETTING RED TEAM TIRE THEMSELVES OUT BY SCORING?
BOLD STRATEGY, BLUE... LET'S SEE IF IT PAYS OFF
imgflip.com

WE CAN REBUILD THEM – WE HAVE THE TRAINING

- Desired goal: “Jacks & Jills of All Trades”
- ANYONE who has hands on keyboard!

- Regardless of issue: ***HANDLE IT***
  - Weaponized carrier files, OSINT, proof-of-execution analysis, etc.

T3: TRAINING THE TRAINERS

- Identify primary resource(s)
- Recognize, assign, and train SMEs
- Hold Trainer the Trainers (T3) sessions

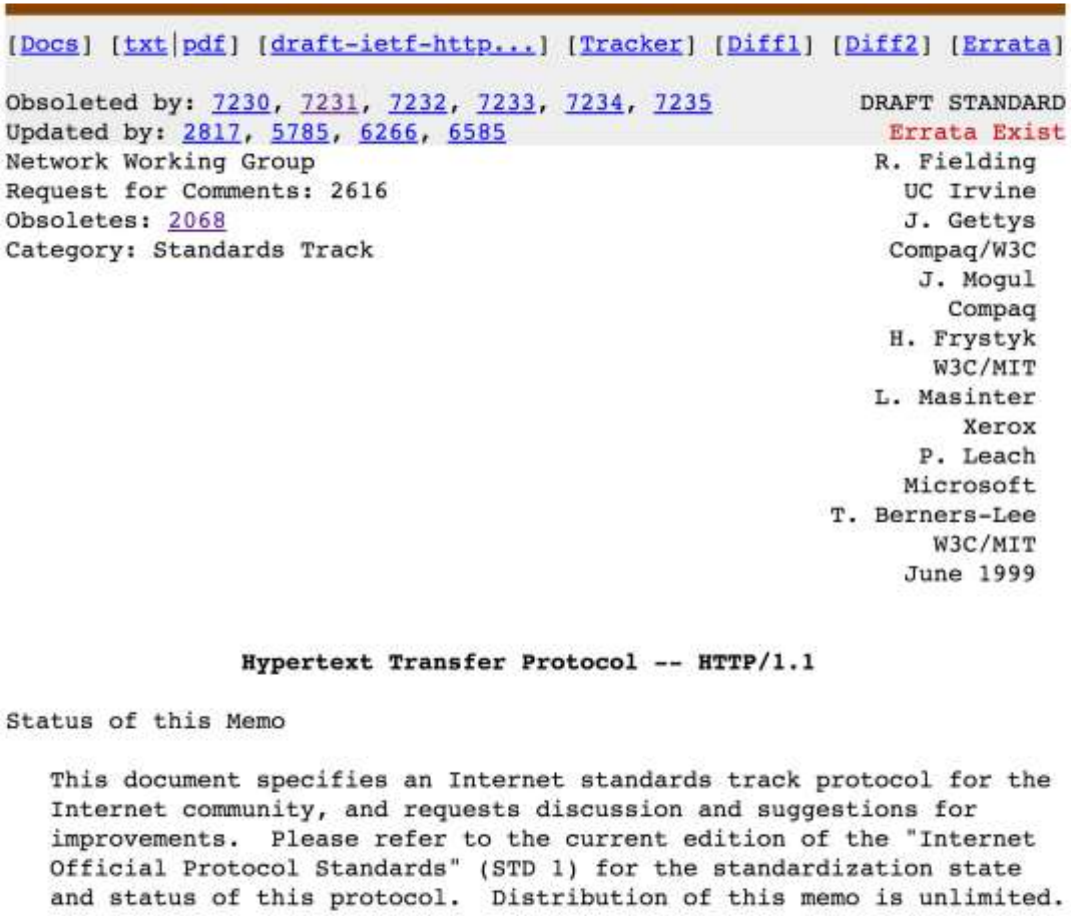
- Example:
  - Primary Trainer → Leads → New-hire analysts

CORE TENANTS

- HOW and WHY
  - No FRU techs!
  - No pressing buttons for bananas!
- Experiential training
  - Hands on the keyboard
  - Kinesthetic learning

CORE TENANTS CONT.

- Foster a "Go here to find…" mentality
- Continually point to reference material
  - Internal documentation
  - External documentation
    - RFCs!!



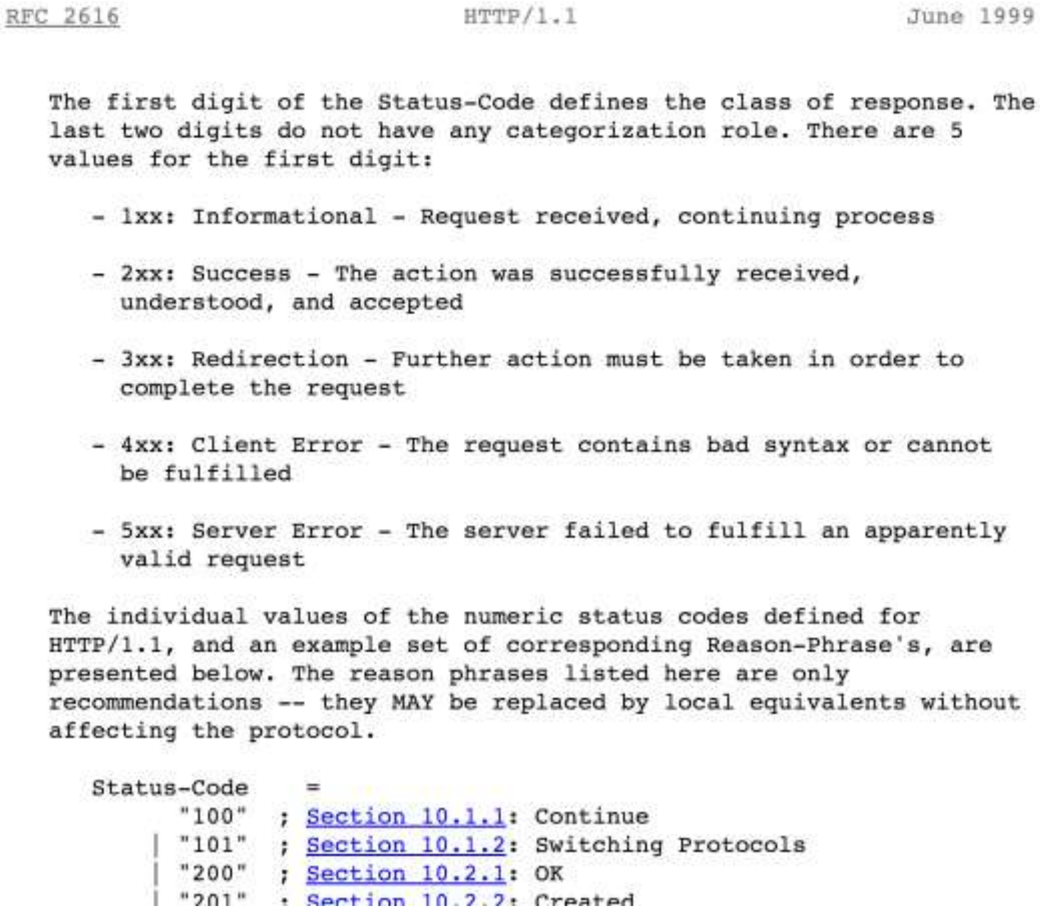
```
[Docs] [txt|pdf] [draft-ietf-http...] [Tracker] [Diff1] [Diff2] [Errata]

Obsoleted by: 7230, 7231, 7232, 7233, 7234, 7235         DRAFT STANDARD
Updated by: 2817, 5785, 6266, 6585                         Errata Exist
Network Working Group                                      R. Fielding
Request for Comments: 2616                                   UC Irvine
Obsoletes: 2068                                              J. Gettys
Category: Standards Track                                   Compaq/W3C
                                                              J. Mogul
                                                                Compaq
                                                            H. Frystyk
                                                               W3C/MIT
                                                           L. Masinter
                                                                 Xerox
                                                              P. Leach
                                                             Microsoft
                                                        T. Berners-Lee
                                                               W3C/MIT
                                                             June 1999


                Hypertext Transfer Protocol -- HTTP/1.1

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.
```



```
RFC 2616                        HTTP/1.1                       June 1999


   The first digit of the Status-Code defines the class of response. The
   last two digits do not have any categorization role. There are 5
   values for the first digit:

      - 1xx: Informational - Request received, continuing process

      - 2xx: Success - The action was successfully received,
        understood, and accepted

      - 3xx: Redirection - Further action must be taken in order to
        complete the request

      - 4xx: Client Error - The request contains bad syntax or cannot
        be fulfilled

      - 5xx: Server Error - The server failed to fulfill an apparently
        valid request

   The individual values of the numeric status codes defined for
   HTTP/1.1, and an example set of corresponding Reason-Phrase's, are
   presented below. The reason phrases listed here are only
   recommendations -- they MAY be replaced by local equivalents without
   affecting the protocol.

      Status-Code    =
            "100"  ; Section 10.1.1: Continue
          | "101"  ; Section 10.1.2: Switching Protocols
          | "200"  ; Section 10.2.1: OK
          | "201"  ; Section 10.2.2: Created
```

CORE TENANTS CONT.

- Take learning styles into account
  - **Kinesthetic** look down
  - Visual look up
  - Auditory look to the sides
- Cover each and every item you run across
  - Ex: Ticket includes obfuscated PowerShell

CORE TENANTS CONT.

- Tie back to the Real World
  - Daily **ticket review** and/or **shadowing**

- Everything ties together in final week
  - Final week should be as hands-on as possible!

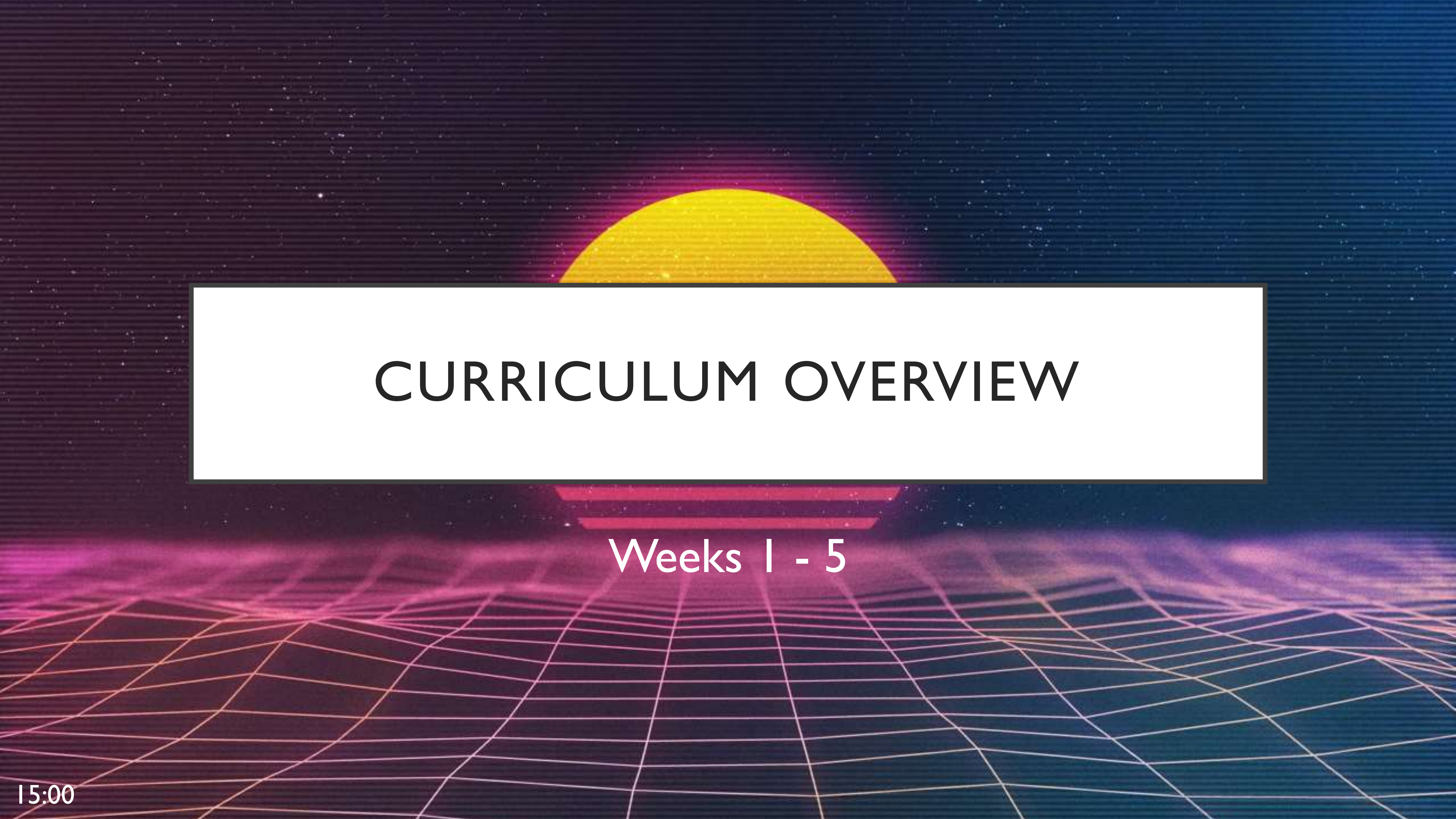
FLEXIBLE FRAMEWORK

BOOTCAMP

- All 5 weeks at once
- Experienced analysts
- May overload new IR analysts

MODULAR

- Multi-phase deployments
- Example:
  - Phase 1: Weeks 1, 2, & 5
  - Phase 2: Week 3 & Week 4
- Easier on new analysts



CURRICULUM OVERVIEW

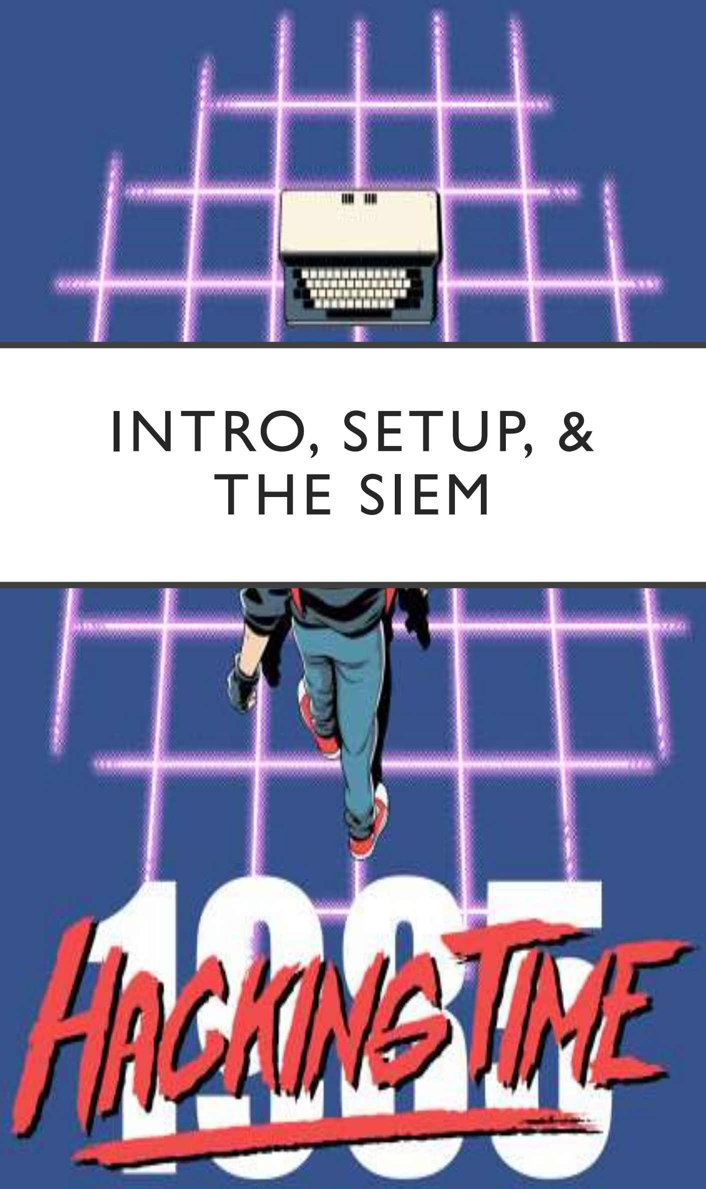
Weeks 1 - 5

15:00

INTRO, SETUP, & THE SIEM

Week 1

INTRO, SETUP, & THE SIEM



- Day 1
  - Company intro & setup
- Day 2-3
  - Setup cont.
- Day 4 & 5
  - The SIEM

TEAM ORIGIN

Precautionary or Reactionary?

Team formation
SOC? CIRT? Tiered? **Why?**

What works?
What **doesn't work?**

(The Good Fight Foundation at Canaan Valley, 2018)

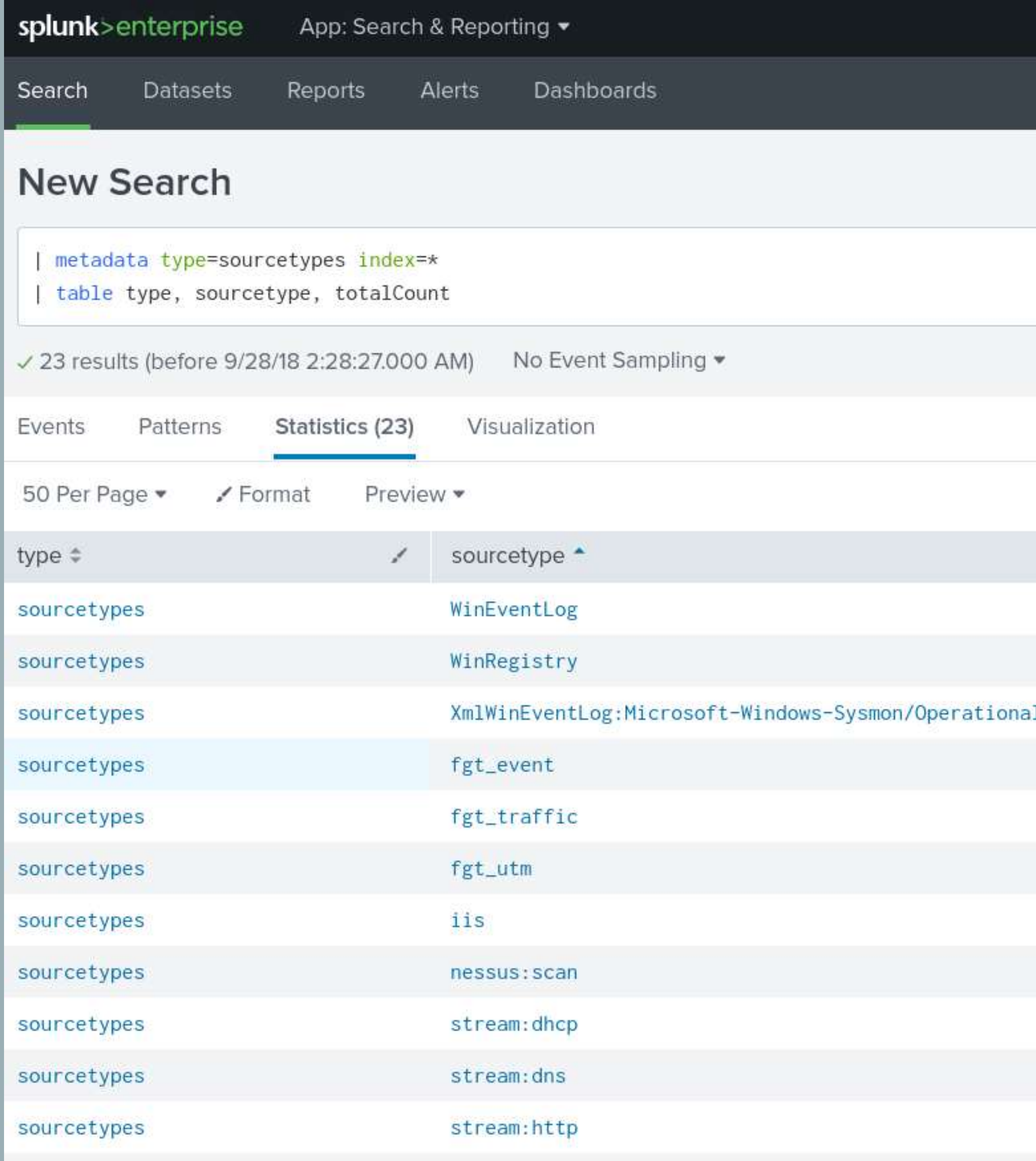
THE SIEM – LOGS

Available data/logs?

Fields?

Documentation?

Known visibility gaps?



New Search

```
| metadata type=sourcetypes index=*
| table type, sourcetype, totalCount
```

✓ 23 results (before 9/28/18 2:28:27.000 AM)

type	sourcetype
sourcetypes	WinEventLog
sourcetypes	WinRegistry
sourcetypes	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetypes	fgt_event
sourcetypes	fgt_traffic
sourcetypes	fgt_utm
sourcetypes	iis
sourcetypes	nessus:scan
sourcetypes	stream:dhcp
sourcetypes	stream:dns
sourcetypes	stream:http

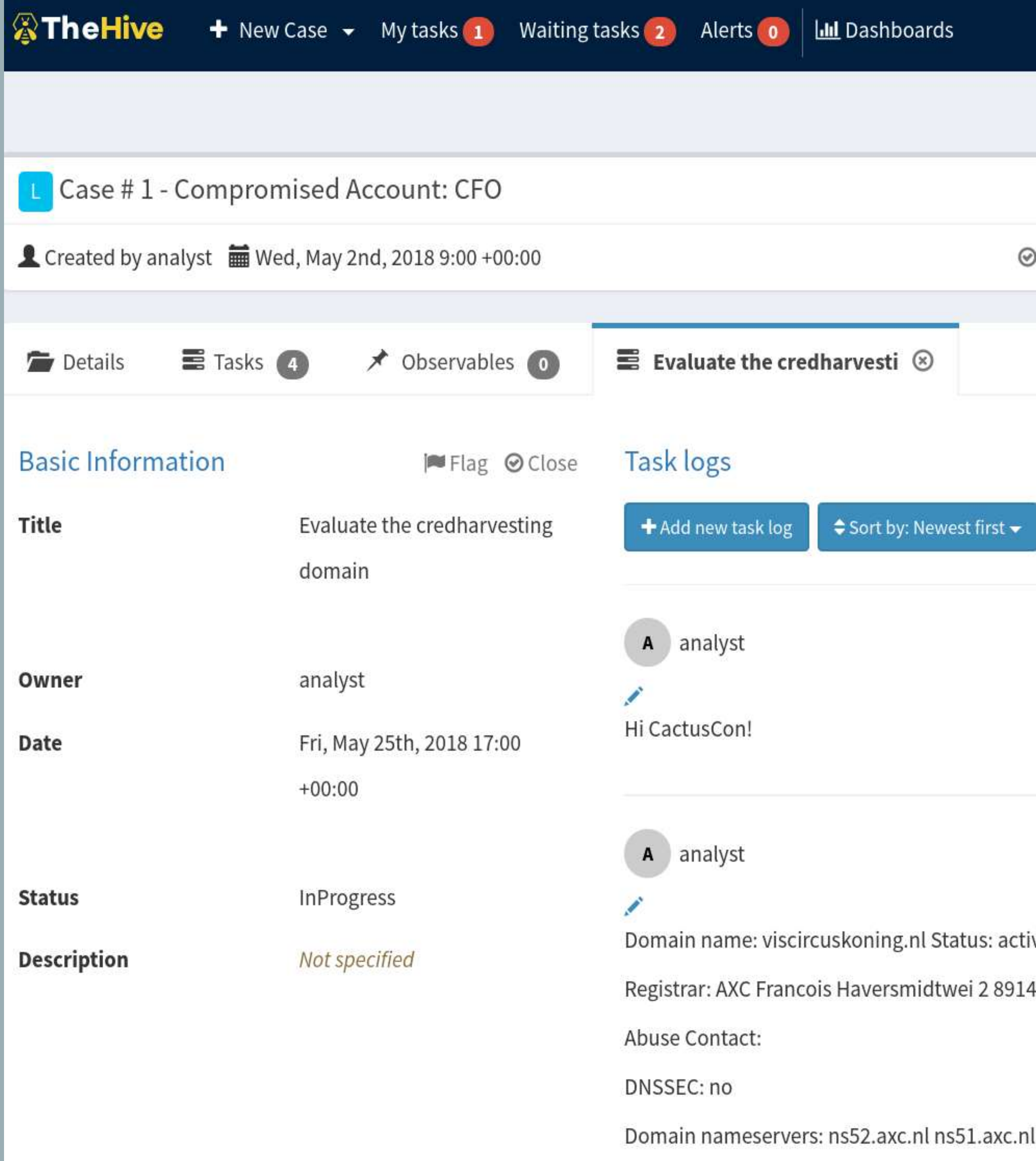
THE SIEM – TICKETS

Fields?

Common ticket types?

Review Top X

Knowledge management?



Case # 1 - Compromised Account: CFO

Created by analyst Wed, May 2nd, 2018 9:00 +00:00

Basic Information

Title Evaluate the credharvesting domain

Owner analyst

Date Fri, May 25th, 2018 17:00 +00:00

Status InProgress

Description *Not specified*

Task logs

analyst

Hi CactusCon!

analyst

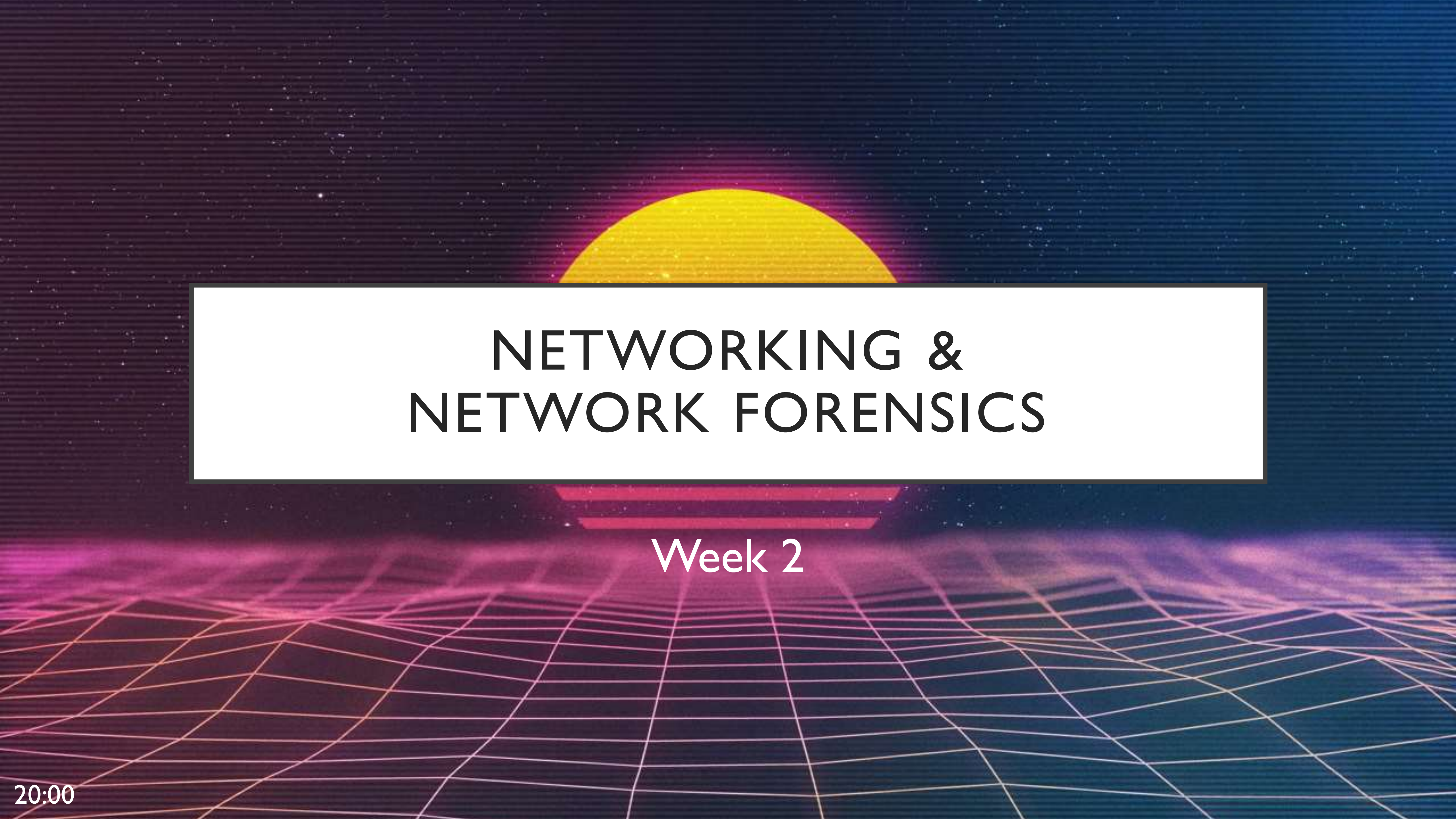
Domain name: viscircuskoning.nl Status: activ

Registrar: AXC Francois Haversmidtwei 2 8914

Abuse Contact:

DNSSEC: no

Domain nameservers: ns52.axc.nl ns51.axc.nl

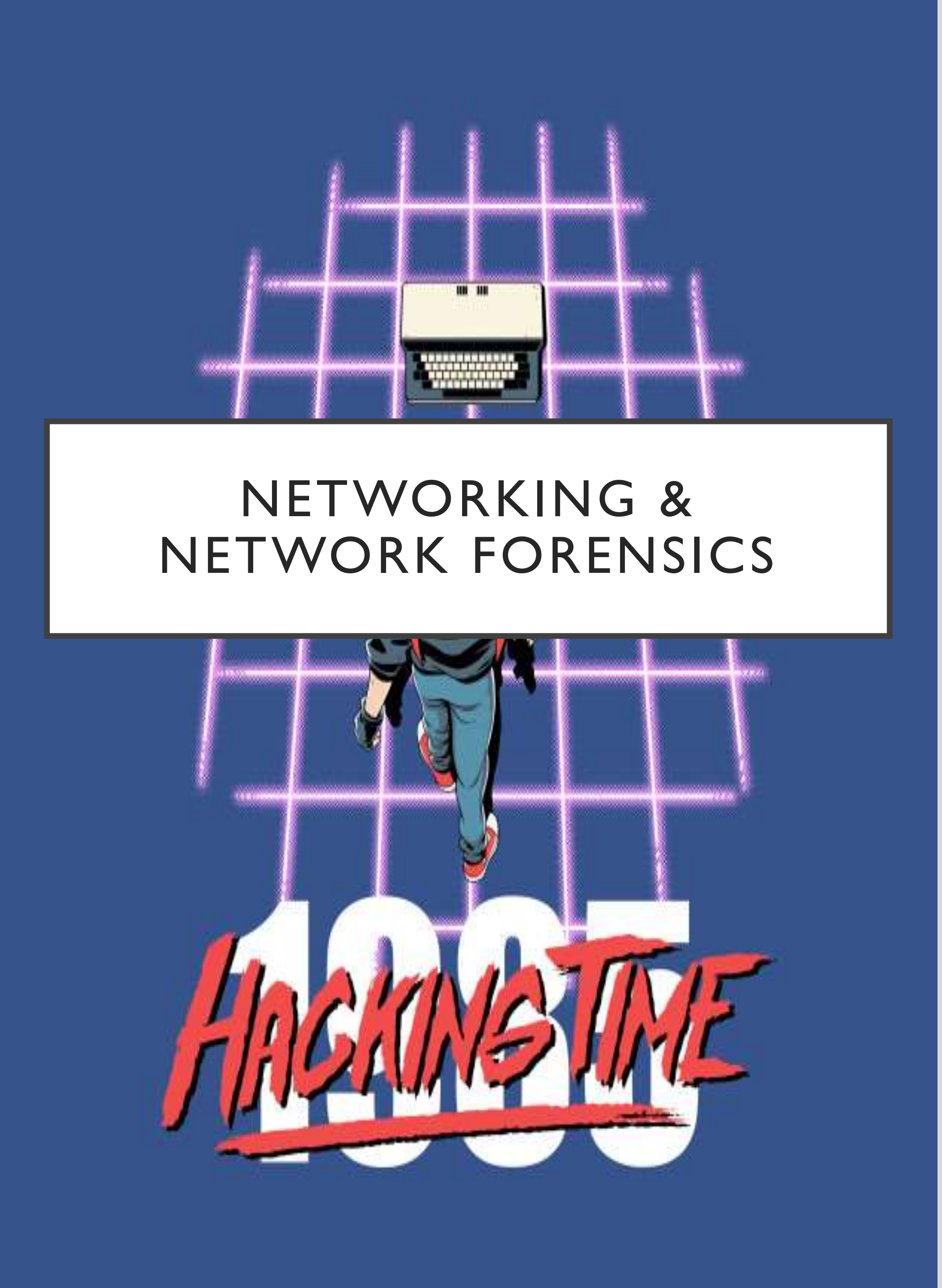


NETWORKING & NETWORK FORENSICS

Week 2

20:00

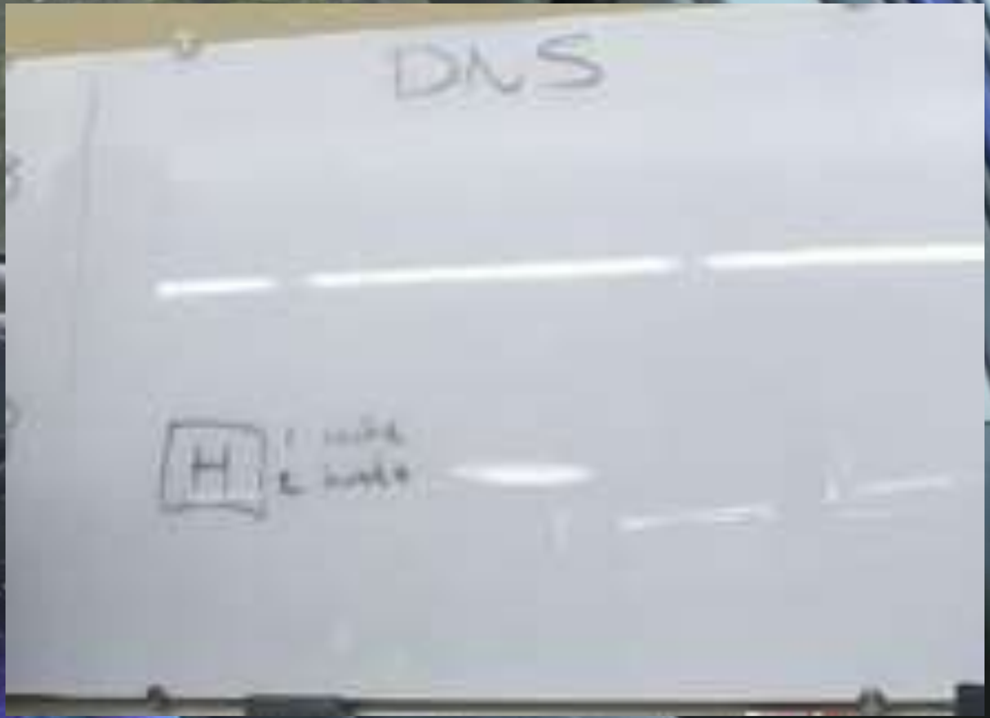
NETWORKING & NETWORK FORENSICS



- Begin w/ network diagram

- Day 1: Common protocols
  - How do they *actually* work?
  - Ex: DNS, HTTP, & SMTP
- Day 2: Network logs
- Day 3: Email
- Day 4: Sanitizing email
- Day 5: Wireshark & PCAP Challenge

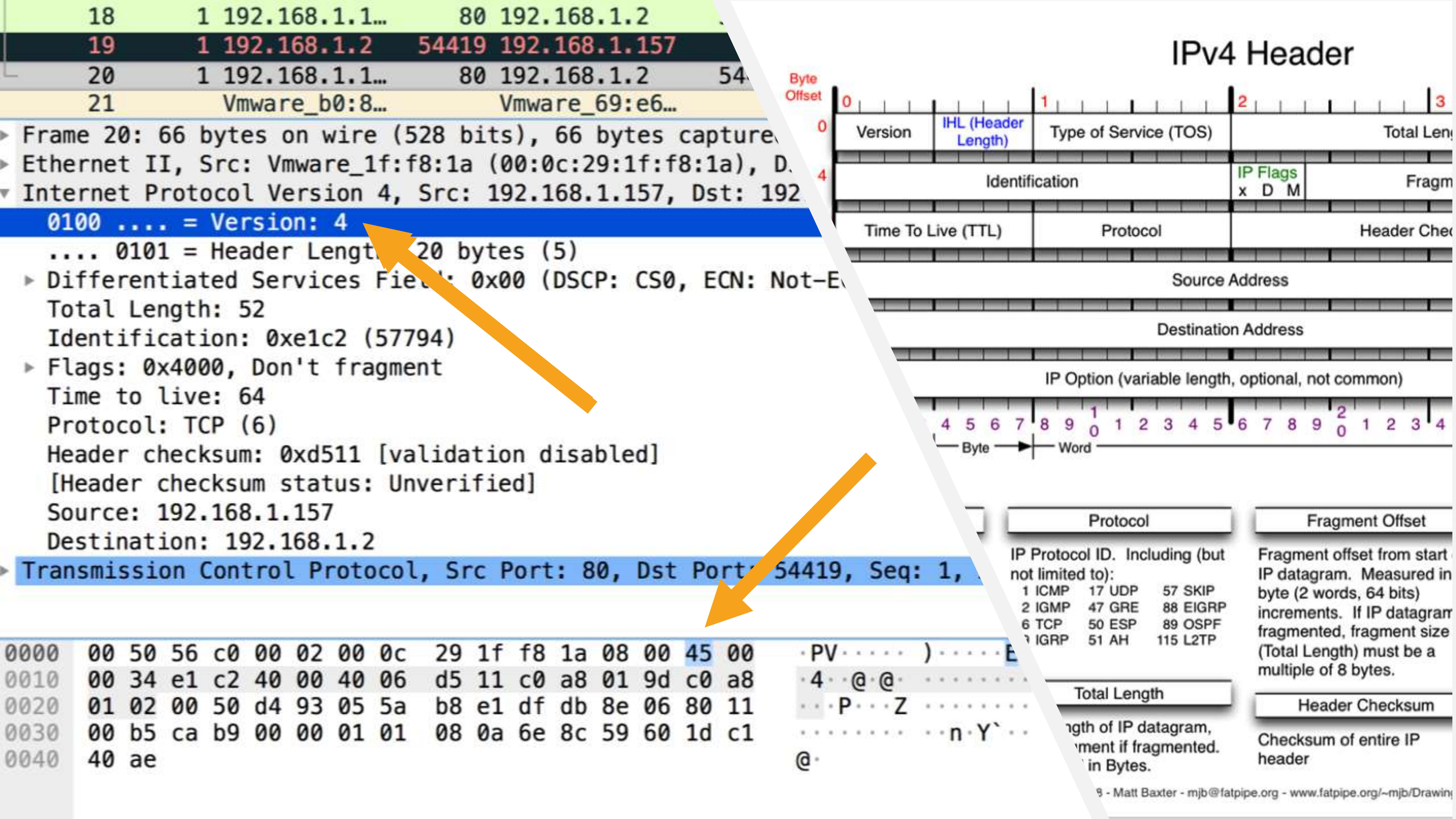
DNS



```
RFC:   RFC 1032-1035 - Domain Names
       RFC 1464 - TXT records
       RFC 1591 - Delegation
       RFC 2219 - CNAME records
etc ...
```

@nillkitty

[illegible] Explains DNS - YouTube



```
18      1 192.168.1.1…      80 192.168.1.2
19      1 192.168.1.2    54419 192.168.1.157
20      1 192.168.1.1…      80 192.168.1.2      54
21        Vmware_b0:8…         Vmware_69:e6…
Frame 20: 66 bytes on wire (528 bits), 66 bytes capture
Ethernet II, Src: Vmware_1f:f8:1a (00:0c:29:1f:f8:1a), D
Internet Protocol Version 4, Src: 192.168.1.157, Dst: 192
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E
    Total Length: 52
    Identification: 0xe1c2 (57794)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd511 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.157
    Destination: 192.168.1.2
Transmission Control Protocol, Src Port: 80, Dst Port: 54419, Seq: 1,

0000  00 50 56 c0 00 02 00 0c  29 1f f8 1a 08 00 45 00   ·PV·····)·····E
0010  00 34 e1 c2 40 00 40 06  d5 11 c0 a8 01 9d c0 a8   ·4··@·@·········
0020  01 02 00 50 d4 93 05 5a  b8 e1 df db 8e 06 80 11   ···P···Z········
0030  00 b5 ca b9 00 00 01 01  08 0a 6e 8c 59 60 1d c1   ··········n·Y`··
0040  40 ae                                              @·
```

IPv4 Header

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Fragment Offset

Fragment offset from start IP datagram. Measured in byte (2 words, 64 bits) increments. If IP datagram fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Total Length

ngth of IP datagram, ment if fragmented. in Bytes.

Header Checksum

Checksum of entire IP header

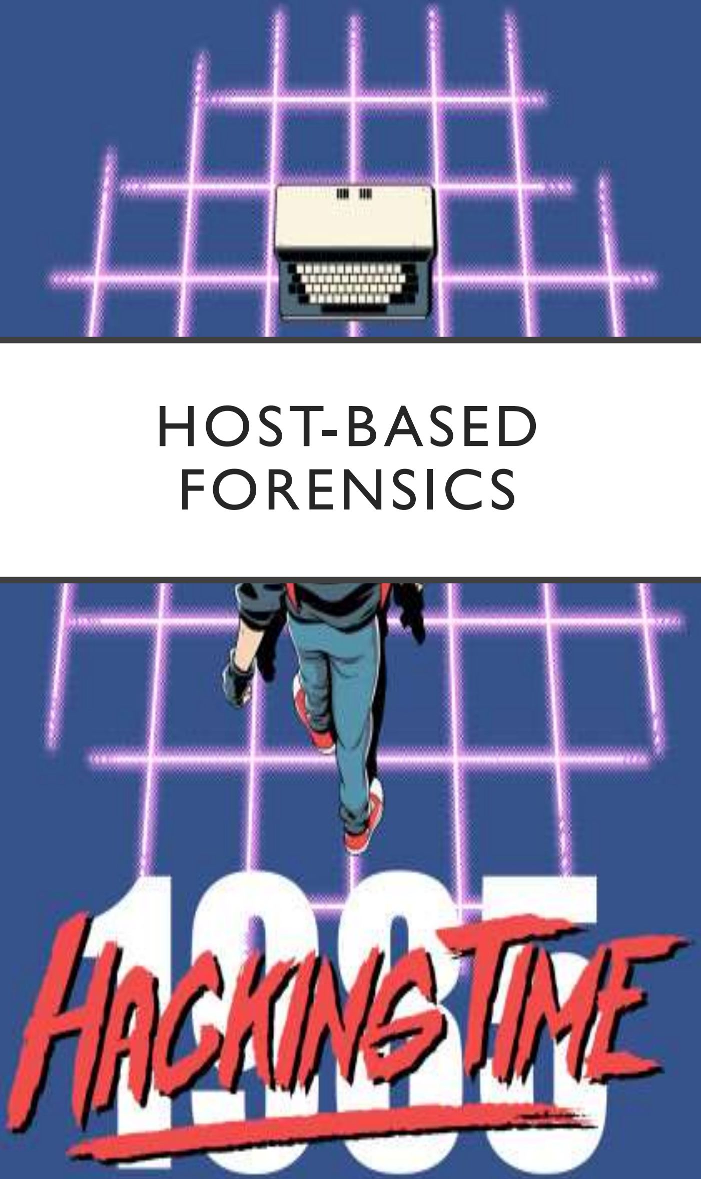
8 - Matt Baxter - mjb@fatpipe.org - www.fatpipe.org/~mjb/Drawin

HOST-BASED FORENSICS

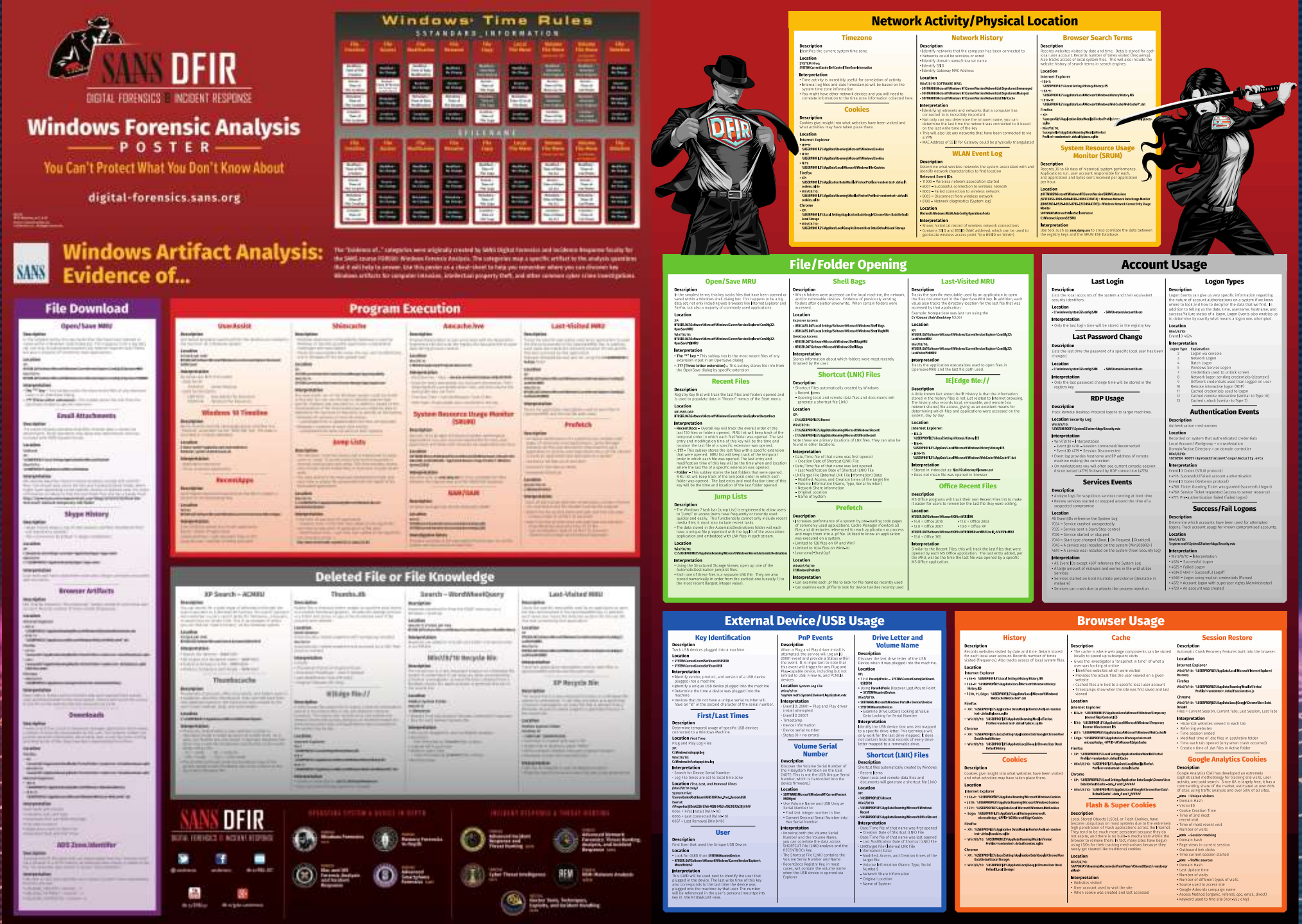
Week 3

25:00

HOST-BASED FORENSICS



- Day 1: Windows artifacts
  - Start with NTFS’ $MFT
- Day 2: Registry analysis cont.
- Day 3: Corp. forensic tool(s)
- Day 4: Eric Zimmerman Tools
- Day 5: Memory analysis deep-dive
  - volatility ftw



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Windows Forensic Analysis POSTER

You Can't Protect What You Don't Know About

digital-forensics.sans.org

Windows Time Rules

$STANDARD_INFORMATION

$FILENAME

Windows Artifact Analysis: Evidence of...

The "Evidence of..." categories were originally created by SANS Digital Forensics and Incident Response faculty for the SANS course FOR500: Windows Forensic Analysis. The categories map a specific artifact to the analysis questions that it will help to answer. Use this poster as a cheat-sheet to help you remember where you can discover key Windows artifacts for computer intrusion, intellectual property theft, and other common cyber crime investigations.

File Download

Open/Save MRU

Email Attachments

Skype History

Browser Artifacts

Downloads

ADS Zone.Identifier

Program Execution

UserAssist

Shimcache

Amcache.hve

Last-Visited MRU

Windows 10 Timeline

System Resource Usage Monitor (SRUM)

Prefetch

RecentApps

Jump Lists

BAM/DAM

Deleted File or File Knowledge

XP Search – ACMRU

Thumbs.db

Search – WordWheelQuery

Last-Visited MRU

Thumbcache

Win7/8/10 Recycle Bin

IE|Edge file://

XP Recycle Bin

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

OPERATING SYSTEM & DEVICE IN-DEPTH

INCIDENT RESPONSE & THREAT HUNTING

Network Activity/Physical Location

Timezone

Description

Identifies the current system time zone.

Location

SYSTEM Hive:
SYSTEM\CurrentControlSet\Control\TimeZoneInformation

Interpretation

- Time activity is incredibly useful for correlation of activity
- Internal log files and date/timestamps will be based on the system time zone information
- You might have other network devices and you will need to correlate information to the time zone information collected here.

Cookies

Description

Cookies give insight into what websites have been visited and what activities may have taken place there.

Location

Internet Explorer

- IE6-8:
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- IE10:
  %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- IE11:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies

Firefox

- XP:
  %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite
- Win7/8/10:
  %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite

Chrome

- XP:
  %USERPROFILE%\Local Settings\ApplicationData\Google\Chrome\User Data\Default\Local Storage
- Win7/8/10:
  %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage

Network History

Description

- Identify networks that the computer has been connected to
- Networks could be wireless or wired
- Identify domain name/intranet name
- Identify SSID
- Identify Gateway MAC Address

Location

Win7/8/10 SOFTWARE HIVE:

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

Interpretation

- Identifying intranets and networks that a computer has connected to is incredibly important
- Not only can you determine the intranet name, you can determine the last time the network was connected to it based on the last write time of the key
- This will also list any networks that have been connected to via a VPN
- MAC Address of SSID for Gateway could be physically triangulated

WLAN Event Log

Description

Determine what wireless networks the system associated with and identify network characteristics to find location

Relevant Event IDs

- 11000 – Wireless network association started
- 8001 – Successful connection to wireless network
- 8002 – Failed connection to wireless network
- 8003 – Disconnect from wireless network
- 6100 – Network diagnostics (System log)

Location

Microsoft-Windows-WLAN-AutoConfig Operational.evtx

Interpretation

- Shows historical record of wireless network connections
- Contains SSID and BSSID (MAC address), which can be used to geolocate wireless access point *(no BSSID on Win8+)

Browser Search Terms

Description

Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files. This will also include the website history of search terms in search engines.

Location

Internet Explorer

- IE6-7:
  %USERPROFILE%\Local Settings\History\History.IE5
- IE8-9:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5
- IE10-11:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Firefox

- XP:
  %userprofile%\Application Data\Mozilla\Firefox\Profiles\<ra [illegible] ault\places.sqlite
- Win7/8/10:
  %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\places.sqlite

System Resource Usage Monitor (SRUM)

Description

Records 30 to 60 days of historical system performance. Applications run, user account responsible for each, and application and bytes sent/received per application per hour.

Location

SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SRUM\Extensions
{973F5D5C-1D90-4944-BE8E-24B94231A174} = Windows Network Data Usage Monitor
{DD6636C4-8929-4683-974E-22C046A43763} = Windows Network Connectivity Usage Monitor
SOFTWARE\Microsoft\WlanSvc\Interfaces\
C:\Windows\System32\SRU\

Interpretation

Use tool such as **srum_dump.exe** to cross correlate the data between the registry keys and the SRUM ESE Database.

File/Folder Opening

Open/Save MRU

Description

In the simplest terms, this key tracks files that have been opened or saved within a Windows shell dialog box. This happens to be a big data set, not only including web browsers like Internet Explorer and Firefox, but also a majority of commonly used applications.

Location

XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU

Interpretation

- **The "*" key –** This subkey tracks the most recent files of any extension input in an OpenSave dialog
- **.??? (Three letter extension) –** This subkey stores file info from the OpenSave dialog by specific extension

Recent Files

Description

Registry Key that will track the last files and folders opened and is used to populate data in "Recent" menus of the Start menu.

Location

NTUSER.DAT:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Interpretation

- **RecentDocs –** Overall key will track the overall order of the last 150 files or folders opened. MRU list will keep track of the temporal order in which each file/folder was opened. The last entry and modification time of this key will be the time and location the last file of a specific extension was opened.
- **.??? –** This subkey stores the last files with a specific extension that were opened. MRU list will keep track of the temporal order in which each file was opened. The last entry and modification time of this key will be the time when and location where the last file of a specific extension was opened.
- **Folder –** This subkey stores the last folders that were opened. MRU list will keep track of the temporal order in which each folder was opened. The last entry and modification time of this key will be the time and location of the last folder opened.

Jump Lists

Description

- The Windows 7 task bar (Jump List) is engineered to allow users to "jump" or access items have frequently or recently used quickly and easily. This functionality cannot only include recent media files; it must also include recent tasks.
- The data stored in the AutomaticDestinations folder will each have a unique file prepended with the AppID of the association application and embedded with LNK files in each stream.

Location

Win7/8/10:
C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

Interpretation

- Using the Structured Storage Viewer, open up one of the AutomaticDestination jumplist files.
- Each one of these files is a separate LNK file. They are also stored numerically in order from the earliest one (usually 1) to the most recent (largest integer value).

Shell Bags

Description

- Which folders were accessed on the local machine, the network, and/or removable devices. Evidence of previously existing folders after deletion/overwrite. When certain folders were accessed.

Location

Explorer Access:

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Desktop Access:

- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

Interpretation

Stores information about which folders were most recently browsed by the user.

Shortcut (LNK) Files

Description

- Shortcut Files automatically created by Windows
  - Recent Items
  - Opening local and remote data files and documents will generate a shortcut file (.lnk)

Location

XP:

- C:\%USERPROFILE%\Recent

Win7/8/10:

- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\
- C:\%USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent\

Note these are primary locations of LNK files. They can also be found in other locations.

Interpretation

- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNKTarget File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System

Prefetch

Description

- Increases performance of a system by pre-loading code pages of commonly used applications. Cache Manager monitors all files and directories referenced for each application or process and maps them into a .pf file. Utilized to know an application was executed on a system.
- Limited to 128 files on XP and Win7
- Limited to 1024 files on Win8-10
- (exename)-(hash).pf

Location

WinXP/7/8/10:
C:\Windows\Prefetch

Interpretation

- Can examine each .pf file to look for file handles recently used
- Can examine each .pf file to look for device handles recently used

Last-Visited MRU

Description

Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.

Example: Notepad.exe was last run using the `C:\Users\Rob\Desktop` folder

Location

XP:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

Win7/8/10:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

Interpretation

Tracks the application executables used to open files in OpenSaveMRU and the last file path used.

IE|Edge file://

Description

A little known fact about the IE History is that the information stored in the history files is not just related to Internet browsing. The history also records local, removable, and remote (via network shares) file access, giving us an excellent means for determining which files and applications were accessed on the system, day by day.

Location

Internet Explorer:

- IE6-7:
  %USERPROFILE%\Local Settings\History\ History.IE5
- IE8-9:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5
- IE10-11:
  %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Interpretation

- Stored in index.dat as: **file:///C:/directory/filename.ext**
- Does not mean file was opened in browser

Office Recent Files

Description

MS Office programs will track their own Recent Files list to make it easier for users to remember the last file they were editing.

Location

NTUSER.DAT\Software\Microsoft\Office\VERSION

- 14.0 = Office 2010
- 12.0 = Office 2007
- 11.0 = Office 2003
- 10.0 = Office XP

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

- 15.0 = Office 365

Interpretation

Similar to the Recent Files, this will track the last files that were opened by each MS Office application. The last entry added, per the MRU, will be the time the last file was opened by a specific MS Office application.

Account Usage

Last Login

Description

Lists the local accounts of the system and their equivalent security identifiers.

Location

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Interpretation

- Only the last login time will be stored in the registry key

Last Password Change

Description

Lists the last time the password of a specific local user has been changed.

Location

- C:\windows\system32\config\SAM
- SAM\Domains\Account\Users

Interpretation

- Only the last password change time will be stored in the registry key

RDP Usage

Description

Track Remote Desktop Protocol logons to target machines.

Location Security Log

Win7/8/10:
%SYSTEM ROOT%\System32\winevt\logs\Security.evtx

Interpretation

- Win7/8/10 – Interpretation
  - Event ID 4778 – Session Connected/Reconnected
  - Event ID 4779 – Session Disconnected
- Event log provides hostname and IP address of remote machine making the connection
- On workstations you will often see current console session disconnected (4779) followed by RDP connection (4778)

Services Events

Description

- Analyze logs for suspicious services running at boot time
- Review services started or stopped around the time of a suspected compromise

Location

All Event IDs reference the System Log

7034 – Service crashed unexpectedly
7035 – Service sent a Start/Stop control
7036 – Service started or stopped
7040 – Start type changed (Boot | On Request | Disabled)
7045 – A service was installed on the system (Win2008R2+)
4697 – A service was installed on the system (from Security log)

Interpretation

- All Event IDs except 4697 reference the System Log
- A large amount of malware and worms in the wild utilize Services
- Services started on boot illustrate persistence (desirable in malware)
- Services can crash due to attacks like process injection

Logon Types

Description

Logon Events can give us very specific information regarding the nature of account authorizations on a system if we know where to look and how to decipher the data that we find. In addition to telling us the date, time, username, hostname, and success/failure status of a logon, Logon Events also enables us to determine by exactly what means a logon was attempted.

Location

Win7/8/10:
Event ID 4624

Interpretation

Logon Type	Explanation
2	Logon via console
3	Network Logon
4	Batch Logon
5	Windows Service Logon
7	Credentials used to unlock screen
8	Network logon sending credentials (cleartext)
9	Different credentials used than logged on user
10	Remote interactive logon (RDP)
11	Cached credentials used to logon
12	Cached remote interactive (similar to Type 10)
13	Cached unlock (similar to Type 7)

Authentication Events

Description

Authentication mechanisms

Location

Recorded on system that authenticated credentials
Local Account/Workgroup = on workstation
Domain/Active Directory = on domain controller

Win7/8/10:
`%SYSTEM ROOT%\System32\winevt\logs\Security.evtx`

Interpretation

Event ID Codes (NTLM protocol)

- 4776: Successful/Failed account authentication

Event ID Codes (Kerberos protocol)

- 4768: Ticket Granting Ticket was granted (successful logon)
- 4769: Service Ticket requested (access to server resource)
- 4771: Pre-authentication failed (failed logon)

Success/Fail Logons

Description

Determine which accounts have been used for attempted logons. Track account usage for known compromised accounts.

Location

Win7/8/10:
%system root%\System32\winevt\logs\Security.evtx

Interpretation

- Win7/8/10 – Interpretation
- 4624 – Successful Logon
- 4625 – Failed Logon
- 4634 | 4647 – Successful Logoff
- 4648 – Logon using explicit credentials (Runas)
- 4672 – Account logon with superuser rights (Administrator)
- 4720 – An account was created

External Device/USB Usage

Key Identification

Description

Track USB devices plugged into a machine.

Location

- SYSTEM\CurrentControlSet\Enum\USBSTOR
- SYSTEM\CurrentControlSet\Enum\USB

Interpretation

- Identify vendor, product, and version of a USB device plugged into a machine
- Identify a unique USB device plugged into the machine
- Determine the time a device was plugged into the machine
- Devices that do not have a unique serial number will have an "&" in the second character of the serial number.

First/Last Times

Description

Determine temporal usage of specific USB devices connected to a Windows Machine.

Location *First Time*

Plug and Play Log Files

XP:
C:\Windows\setupapi.log

Win7/8/10:
C:\Windows\inf\setupapi.dev.log

Interpretation

- Search for Device Serial Number
- Log File times are set to local time zone

Location *First, Last, and Removal Times (Win7/8/10 Only)*

System Hive:
\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USB iSerial:
#\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\####

0064 = First Install (Win7-10)
0066 = Last Connected (Win8-10)
0067 = Last Removal (Win8-10)

User

Description

Find User that used the Unique USB Device.

Location

- Look for GUID from **SYSTEM\MountedDevices**
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

Interpretation

This GUID will be used next to identify the user that plugged in the device. The last write time of this key also corresponds to the last time the device was plugged into the machine by that user. The number will be referenced in the user's personal mountpoints key in the NTUSER.DAT Hive.

PnP Events

Description

When a Plug and Play driver install is attempted, the service will log an ID 20001 event and provide a Status within the event. It is important to note that this event will trigger for any Plug and Play-capable device, including but not limited to USB, Firewire, and PCMCIA devices.

Location *System Log File*

Win7/8/10:
%system root%\System32\winevt\logs\System.evtx

Interpretation

- Event ID: 20001 – Plug and Play driver install attempted
- Event ID 20001
- Timestamp
- Device information
- Device serial number
- Status (0 = no errors)

Volume Serial Number

Description

Discover the Volume Serial Number of the Filesystem Partition on the USB. (NOTE: This is not the USB Unique Serial Number, which is hardcoded into the device firmware.)

Location

- SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ENDMgmt
- Use Volume Name and USB Unique Serial Number to:
  - Find last integer number in line
  - Convert Decimal Serial Number into Hex Serial Number

Interpretation

- Knowing both the Volume Serial Number and the Volume Name, you can correlate the data across SHORTCUT File (LNK) analysis and the RECENTDOCs key.
- The Shortcut File (LNK) contains the Volume Serial Number and Name
- RecentDocs Registry Key, in most cases, will contain the volume name when the USB device is opened via Explorer

Drive Letter and Volume Name

Description

Discover the last drive letter of the USB Device when it was plugged into the machine.

Location

XP:

- Find **ParentIdPrefix – SYSTEM\CurrentControlSet\Enum\USBSTOR**
- Using **ParentIdPrefix** Discover Last Mount Point **– SYSTEM\MountedDevices**

Win7/8/10:

- SOFTWARE\Microsoft\Windows Portable Devices\Devices
- SYSTEM\MountedDevices
  - Examine Drive Letters looking at Value Data Looking for Serial Number

Interpretation

Identify the USB device that was last mapped to a specific drive letter. This technique will only work for the last drive mapped. It does not contain historical records of every drive letter mapped to a removable drive.

Shortcut (LNK) Files

Description

Shortcut files automatically created by Windows

- Recent Items
- Open local and remote data files and documents will generate a shortcut file (.lnk)

Location

XP:

- %USERPROFILE%\Recent

Win7/8/10

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
- %USERPROFILE%\AppData\Roaming\Microsoft\Office\Recent

Interpretation

- Date/Time file of that name was first opened
  - Creation Date of Shortcut (LNK) File
- Date/Time file of that name was last opened
  - Last Modification Date of Shortcut (LNK) File
- LNKTarget File (Internal LNK File Information) Data:
  - Modified, Access, and Creation times of the target file
  - Volume Information (Name, Type, Serial Number)
  - Network Share information
  - Original Location
  - Name of System

Browser Usage

History

Description

Records websites visited by date and time. Details stored for each local user account. Records number of times visited (frequency). Also tracks access of local system files.

Location

Internet Explorer

- IE6-7: %USERPROFILE%\Local Settings\History\History.IE5
- IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\History\History.IE5
- IE10, 11, Edge: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat

Firefox

- XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite
- Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite

Chrome

- XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\History
- Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

Cookies

Description

Cookies give insight into what websites have been visited and what activities may have taken place there.

Location

Internet Explorer

- IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- IE10: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCookies
- Edge: %USERPROFILE%\AppData\Local\Packages\microsoft.microsoftedge_<APPID>\AC\MicrosoftEdge\Cookies

Firefox

- XP: %USERPROFILE%\Application Data\Mozilla\Firefox\Profiles\<random text>.default\cookies.sqlite
- Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\cookies.sqlite

Chrome

- XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Local Storage\
- Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Local Storage\

Cache

Description

- The cache is where web page components can be stored locally to speed up subsequent visits
- Gives the investigator a "snapshot in time" of what a user was looking at online
  - Identifies websites which were visited
  - Provides the actual files the user viewed on a given website
  - Cached files are tied to a specific local user account
  - Timestamps show when the site was first saved and last viewed

Location

Internet Explorer

- IE8-9: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- IE10: %USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
- IE11: %USERPROFILE%\AppData\Local\Microsoft\Windows\INetCache\IE
- Edge: %USERPROFILE%\AppData\Local\Packages\microsoft.microsoftedge_<APPID>\AC\MicrosoftEdge\Cache

Firefox

- XP: %USERPROFILE%\Local Settings\ApplicationData\Mozilla\Firefox\Profiles\<randomtext>.default\Cache
- Win7/8/10: %USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\<randomtext>.default\Cache

Chrome

- XP: %USERPROFILE%\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache - data_# and f_######
- Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\Cache\ - data_# and f_######

Flash & Super Cookies

Description

Local Stored Objects (LSOs), or Flash Cookies, have become ubiquitous on most systems due to the extremely high penetration of Flash applications across the Internet. They tend to be much more persistent because they do not expire, and there is no built-in mechanism within the browser to remove them. In fact, many sites have begun using LSOs for their tracking mechanisms because they rarely get cleared like traditional cookies.

Location

Win7/8/10:
%APPDATA%\Roaming\Macromedia\FlashPlayer\#SharedObjects\<randomprofileid>

Interpretation

- Websites visited
- User account used to visit the site
- When cookie was created and last accessed

Session Restore

Description

Automatic Crash Recovery features built into the browser.

Location

Internet Explorer

Win7/8/10: %USERPROFILE%/AppData/Local/Microsoft/Internet Explorer/Recovery

Firefox

Win7/8/10: %USERPROFILE%\AppData\Roaming\Mozilla\Firefox\Profiles\<randomtext>.default\sessionstore.js

Chrome

Win7/8/10: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\
Files = Current Session, Current Tabs, Last Session, Last Tabs

Interpretation

- Historical websites viewed in each tab
- Referring websites
- Time session ended
- Modified time of .dat files in LastActive folder
- Time each tab opened (only when crash occurred)
- Creation time of .dat files in Active folder

Google Analytics Cookies

Description

Google Analytics (GA) has developed an extremely sophisticated methodology for tracking site visits, user activity, and paid search. Since GA is largely free, it has a commanding share of the market, estimated at over 80% of sites using traffic analysis and over 50% of all sites.

_utma – Unique visitors

- Domain Hash
- Visitor ID
- Cookie Creation Time
- Time of 2nd most recent visit
- Time of most recent visit
- Number of visits

_utmb – Session tracking

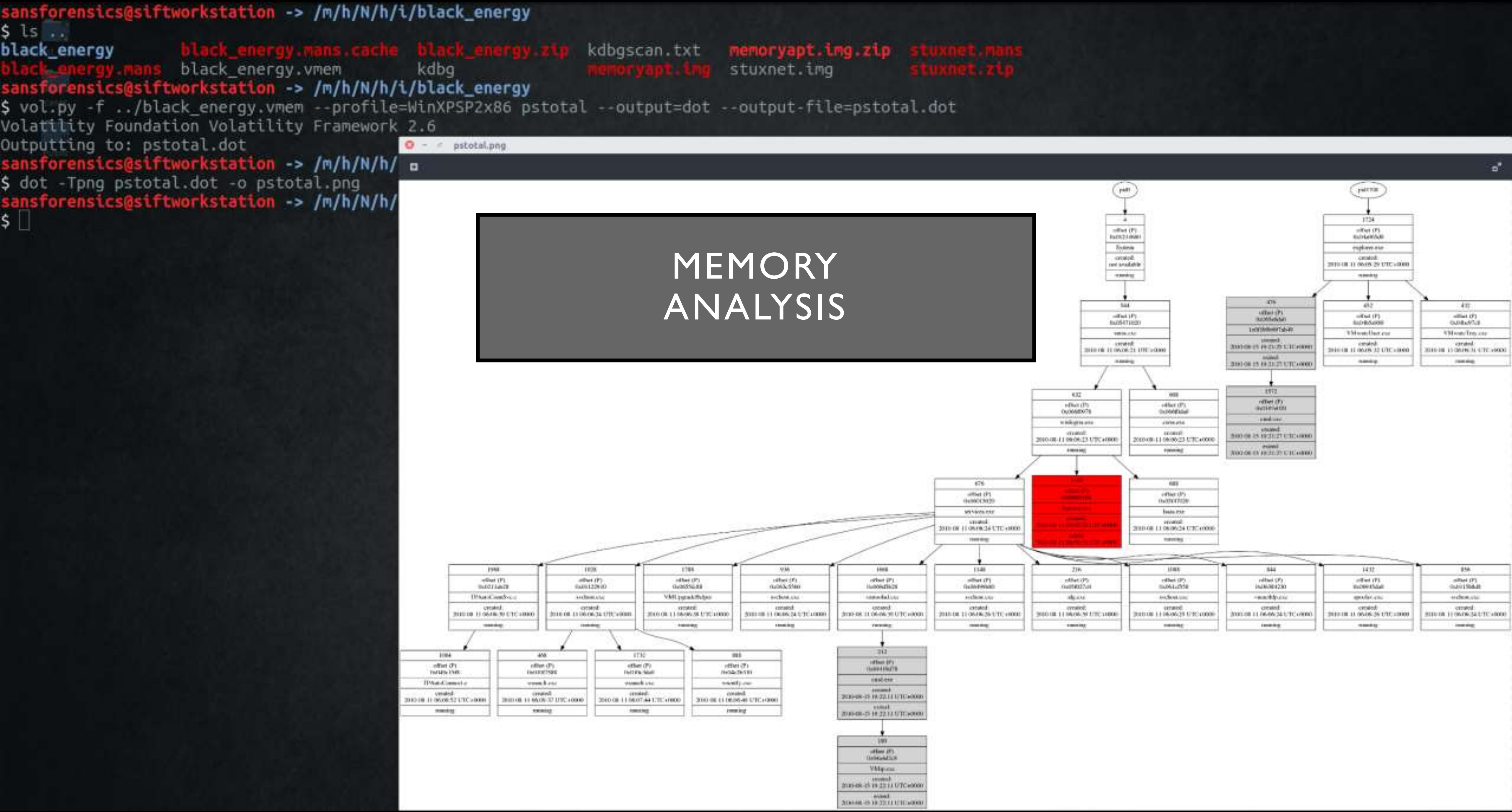
- Domain hash
- Page views in current session
- Outbound link clicks
- Time current session started

_utmz – Traffic sources

- Domain Hash
- Last Update time
- Number of visits
- Number of different types of visits
- Source used to access site
- Google Adwords campaign name
- Access Method (organic, referral, cpc, email, direct)
- Keyword used to find site (non-SSL only)

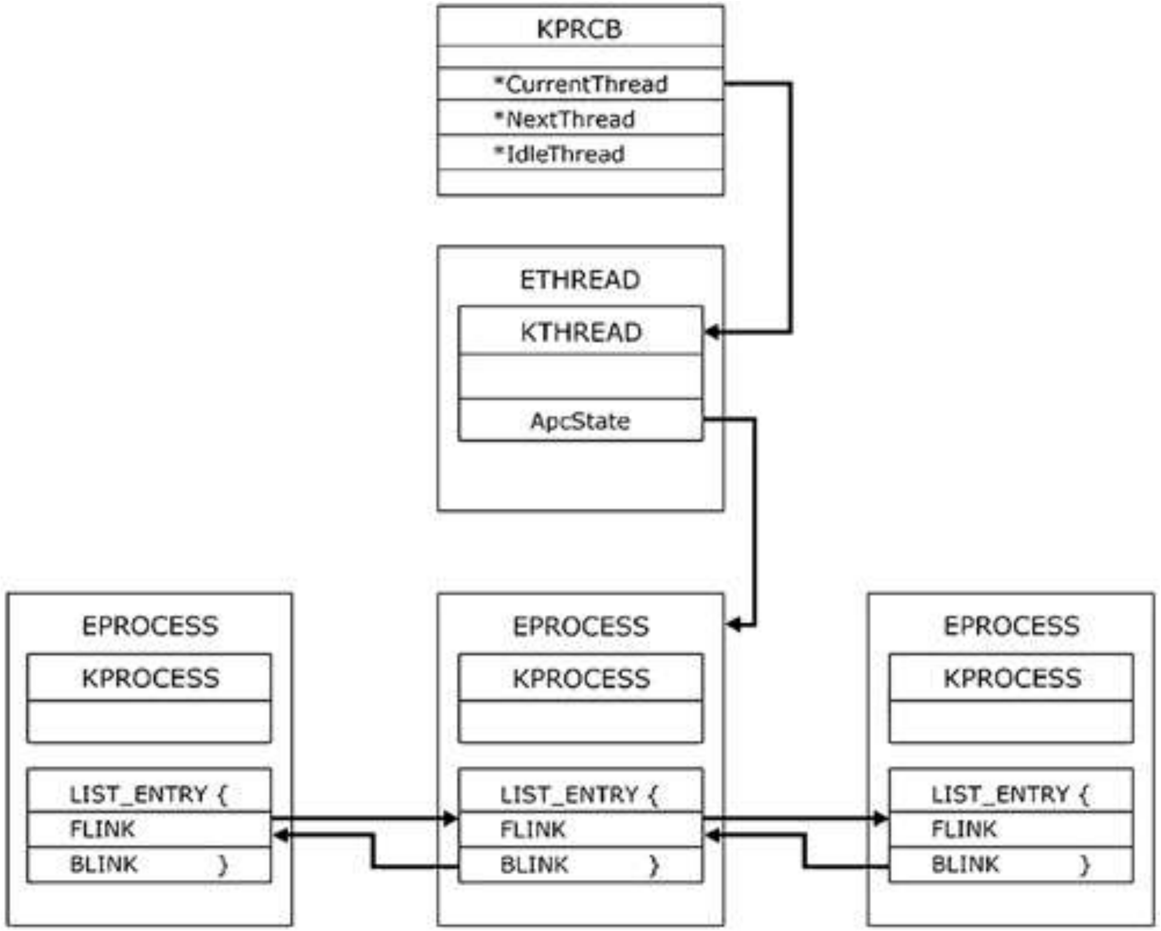
SANS 500

MEMORY ANALYSIS

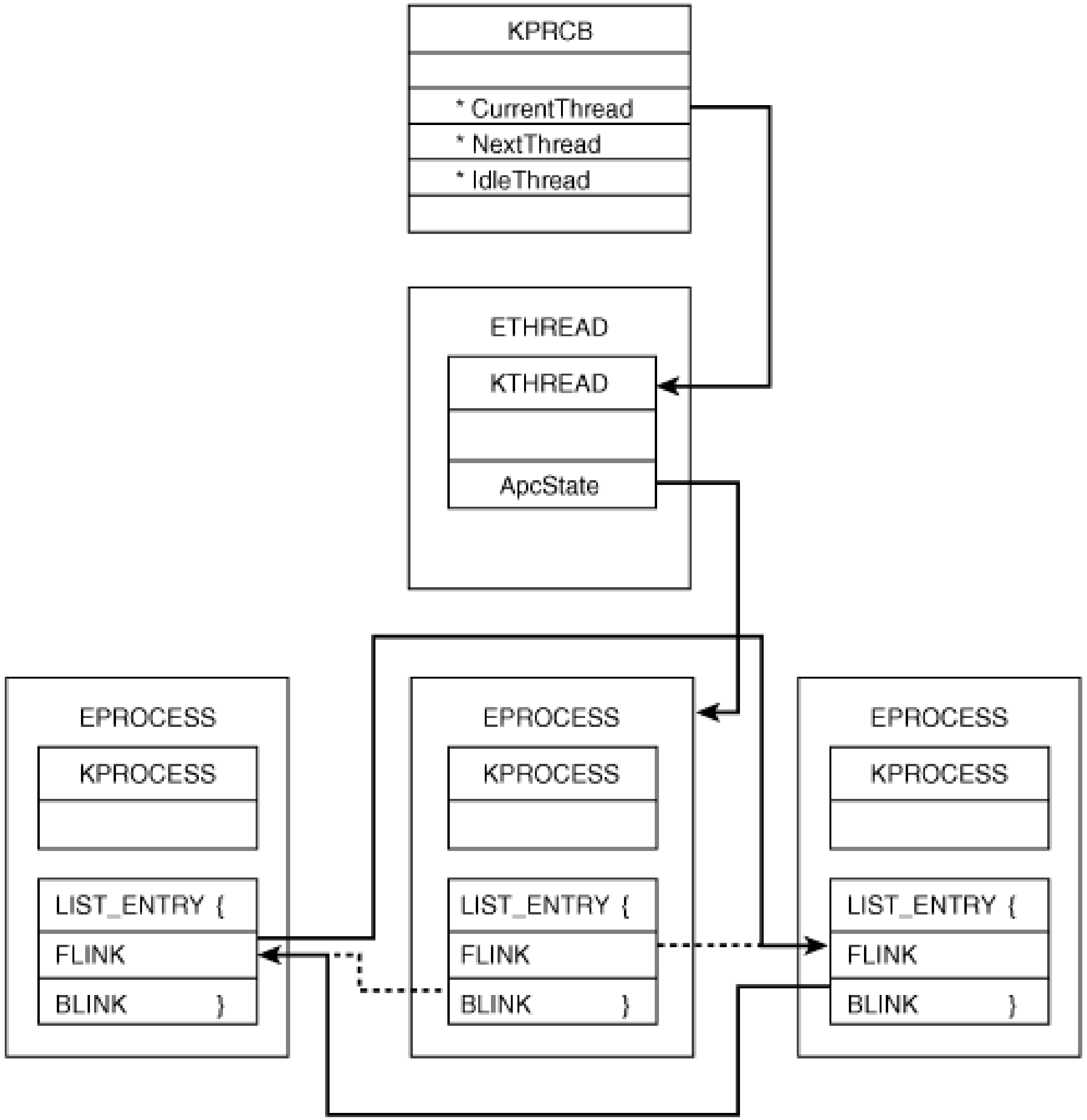


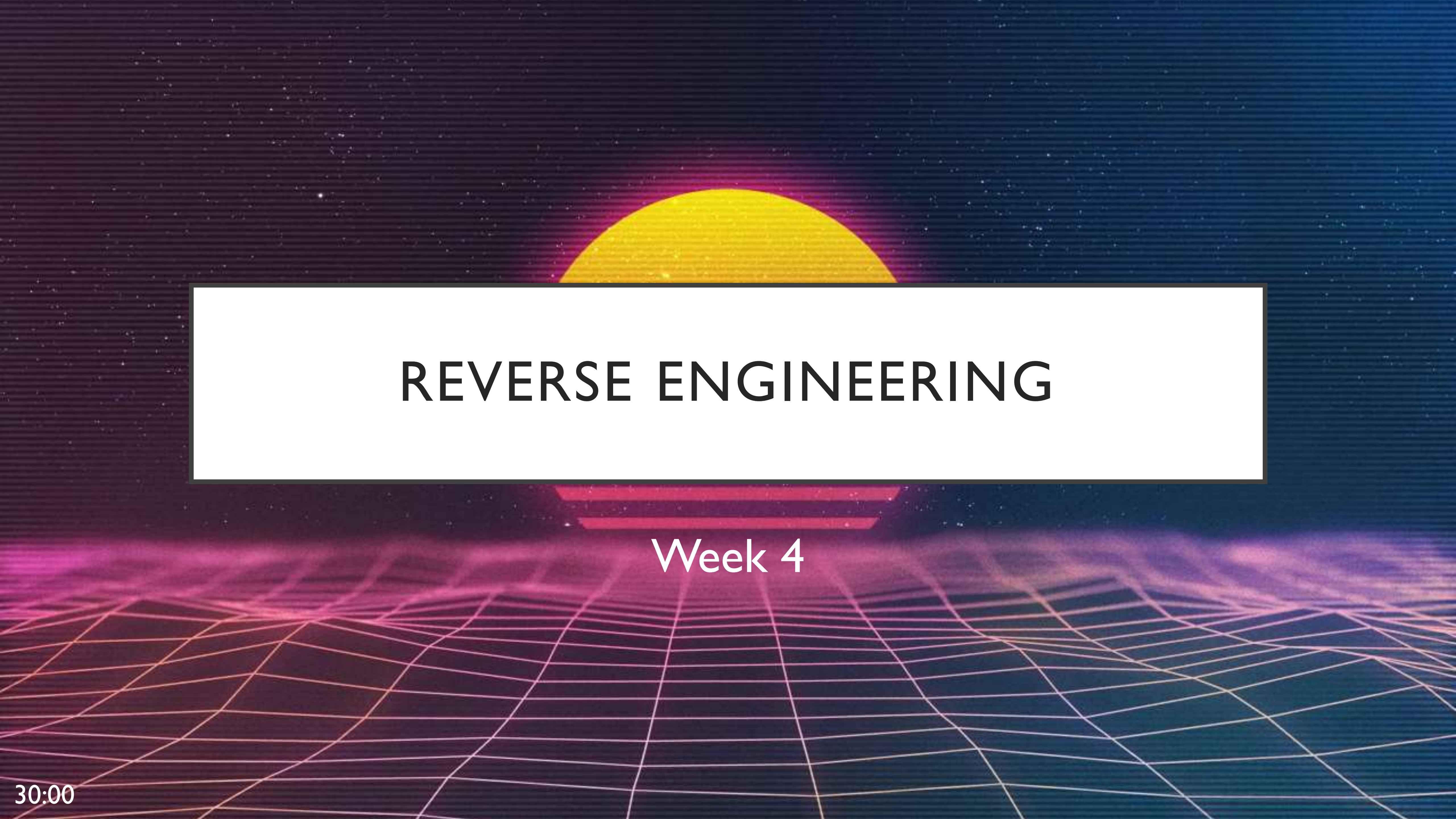
```
sansforensics@siftworkstation -> /m/h/N/h/i/black_energy
$ ls ..
black_energy        black_energy.mans.cache  black_energy.zip  kdbgscan.txt   memoryapt.img.zip  stuxnet.mans
black_energy.mans   black_energy.vmem        kdbg              memoryapt.img  stuxnet.img        stuxnet.zip
sansforensics@siftworkstation -> /m/h/N/h/i/black_energy
$ vol.py -f ../black_energy.vmem --profile=WinXPSP2x86 pstotal --output=dot --output-file=pstotal.dot
Volatility Foundation Volatility Framework 2.6
Outputting to: pstotal.dot
sansforensics@siftworkstation -> /m/h/N/h/
$ dot -Tpng pstotal.dot -o pstotal.png
sansforensics@siftworkstation -> /m/h/N/h/
$ 
```

PSLIST VS. PSSCAN



(Hoglund & Butler, 2005)

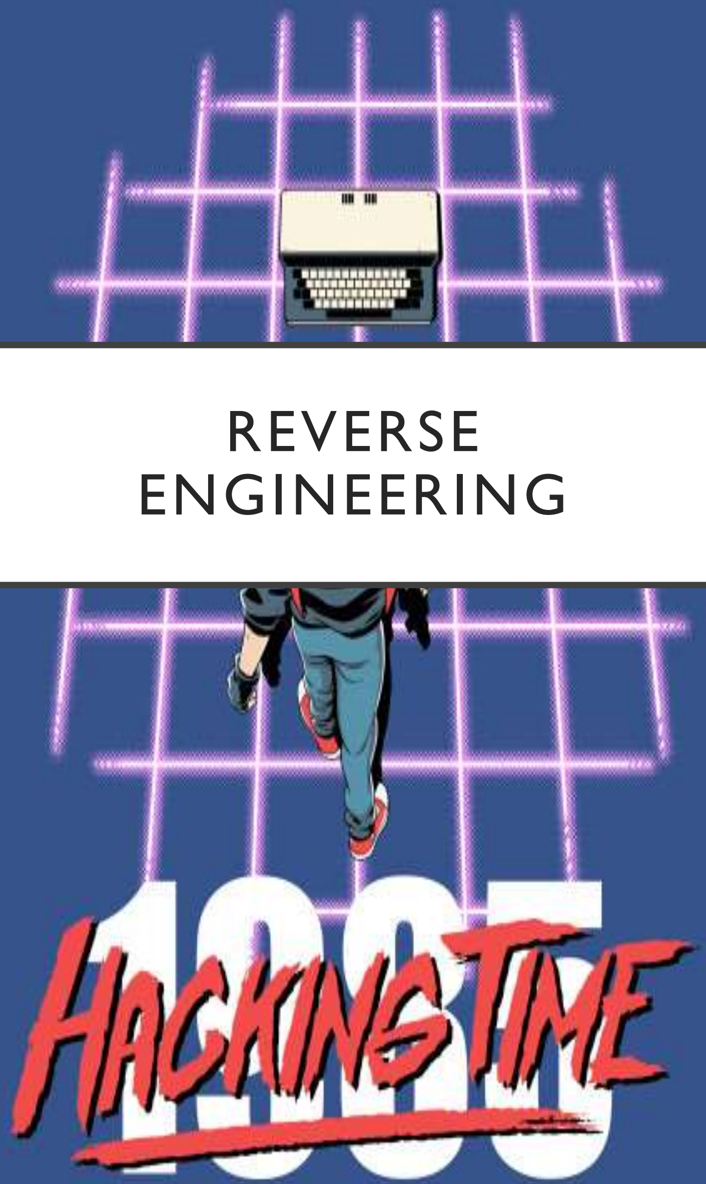




REVERSE ENGINEERING

Week 4

30:00



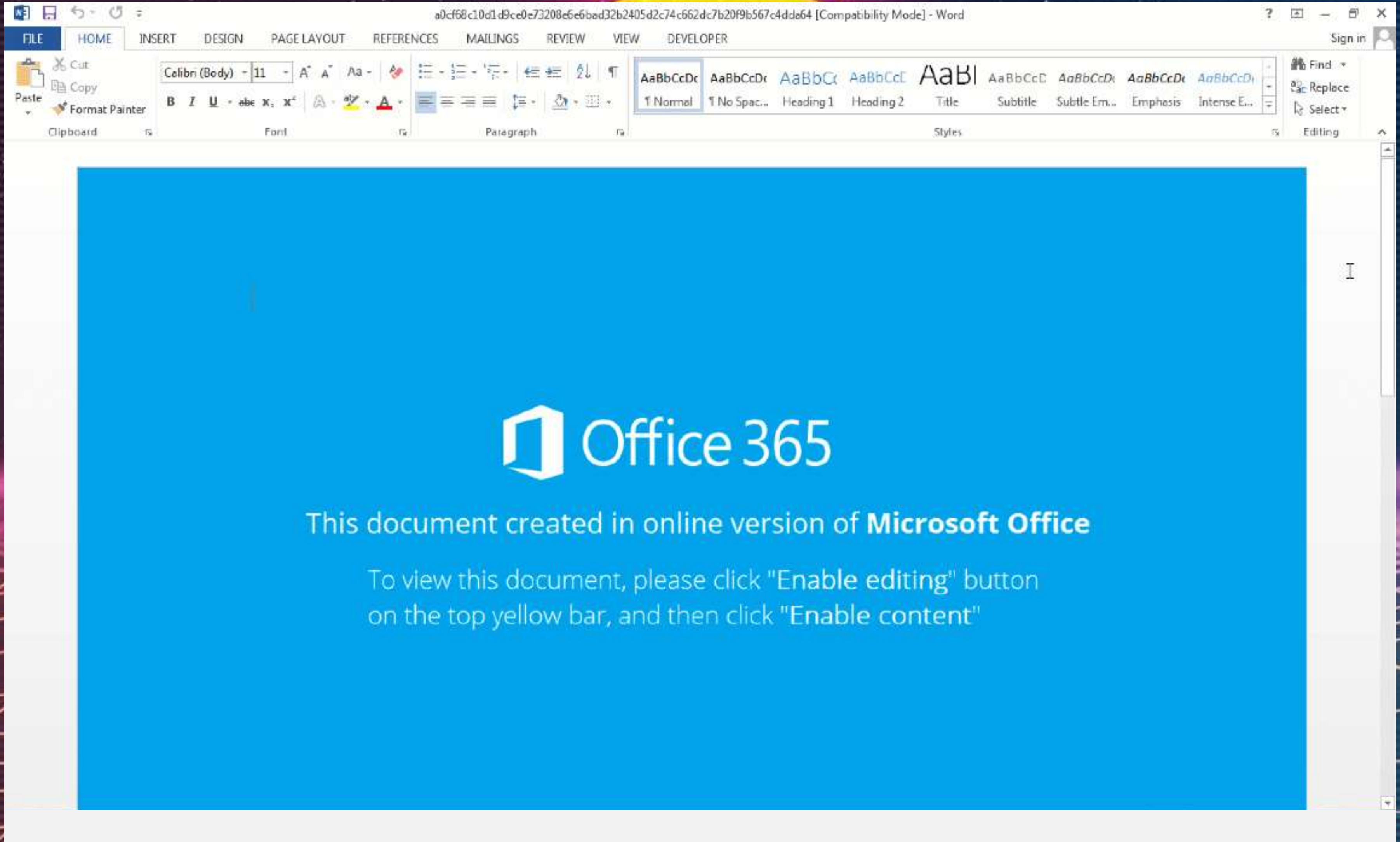
REVERSE ENGINEERING

- Day 1: PDF analysis
- Day 2: Office file analysis

- Day 3: Dynamic PE analysis
- Day 4: Static PE analysis

- Day 5: Sam's Malware Workshop

CARRIER FILE ANALYSIS



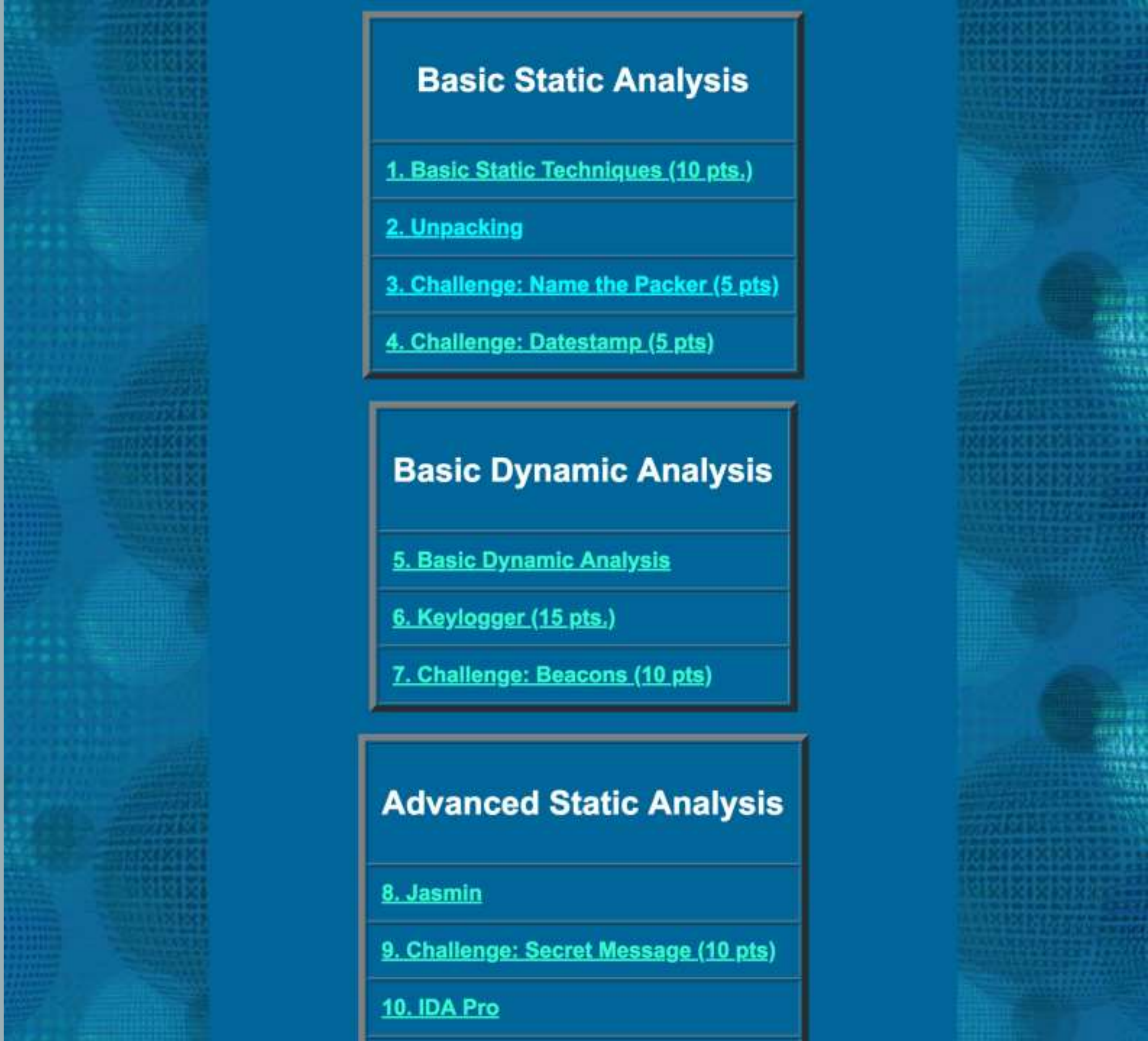
a0cf68c10d1d9ce0e73208e6e6bad32b2405d2c74c662dc7b20f9b567c4dda64 [Compatibility Mode] - Word

This document created in online version of **Microsoft Office**

To view this document, please click "Enable editing" button
on the top yellow bar, and then click "Enable content"

SAM'S MALWARE WORKSHOP

https://samsclass.info/126/126_DC_2017.shtml



Basic Static Analysis

1. Basic Static Techniques (10 pts.)

2. Unpacking

3. Challenge: Name the Packer (5 pts)

4. Challenge: Datestamp (5 pts)

Basic Dynamic Analysis

5. Basic Dynamic Analysis

6. Keylogger (15 pts.)

7. Challenge: Beacons (10 pts)

Advanced Static Analysis

8. Jasmin

9. Challenge: Secret Message (10 pts)

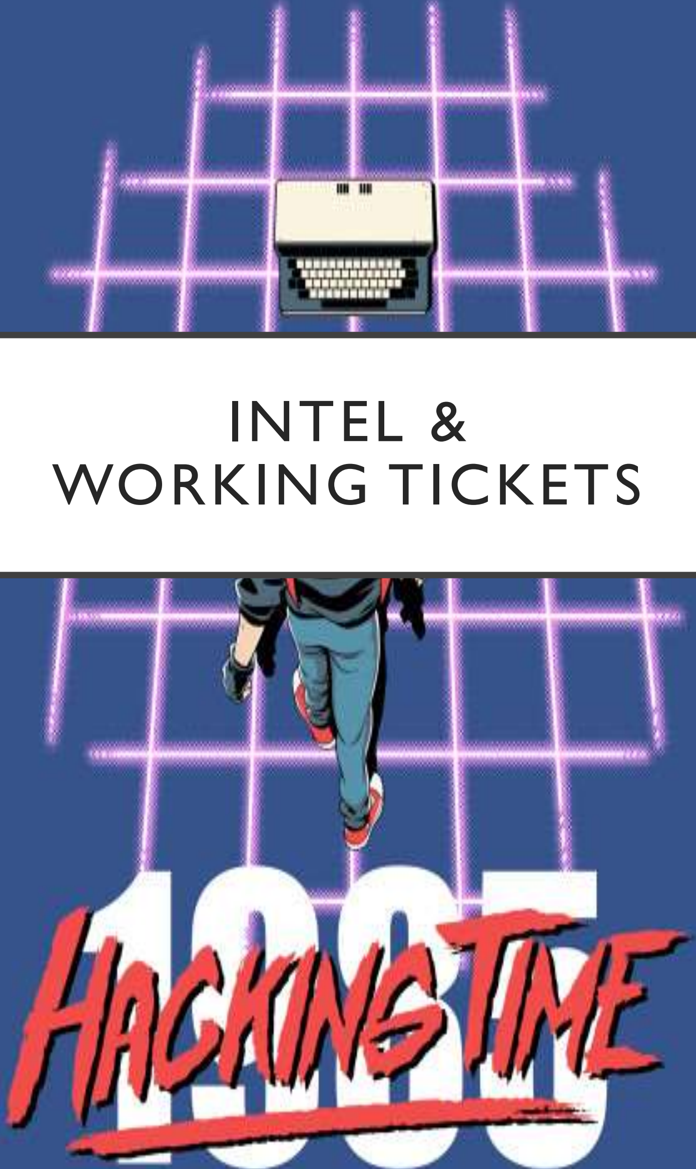
10. IDA Pro

INTEL & WORKING TICKETS

Week 5

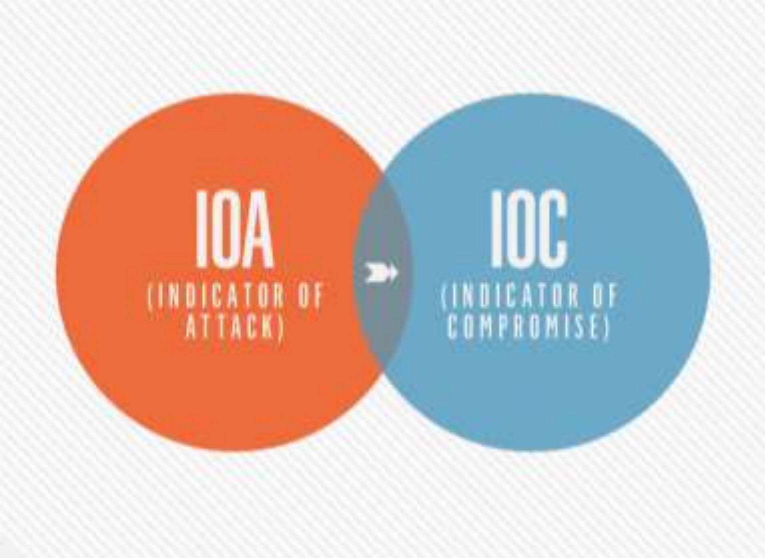
35:00

INTEL & WORKING TICKETS



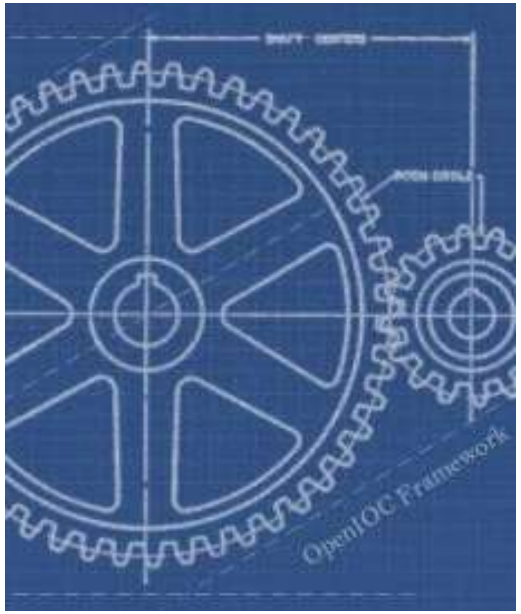
- Day 1: IOCs (& IOAs)
- Day 2: Threat Hunting
- Day 3: Operationalizing OSINT
  - See Pluralsight.com course
- Day 4: Working tickets
- Day 5: Review & Wrap-up

IOCS



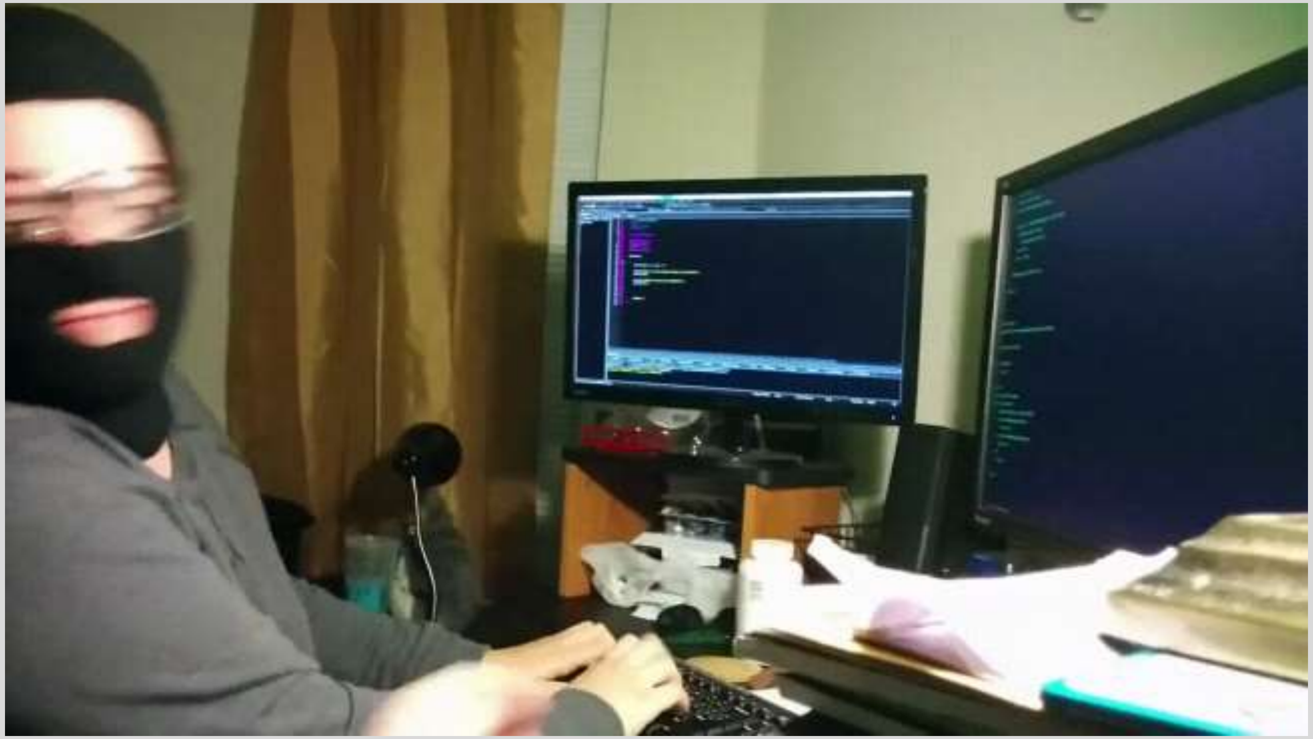
yara

STIX™



THREAT HUNTING

Finding what security tools ***don’t***



What frameworks are YOU using?

REINFORCEMENT

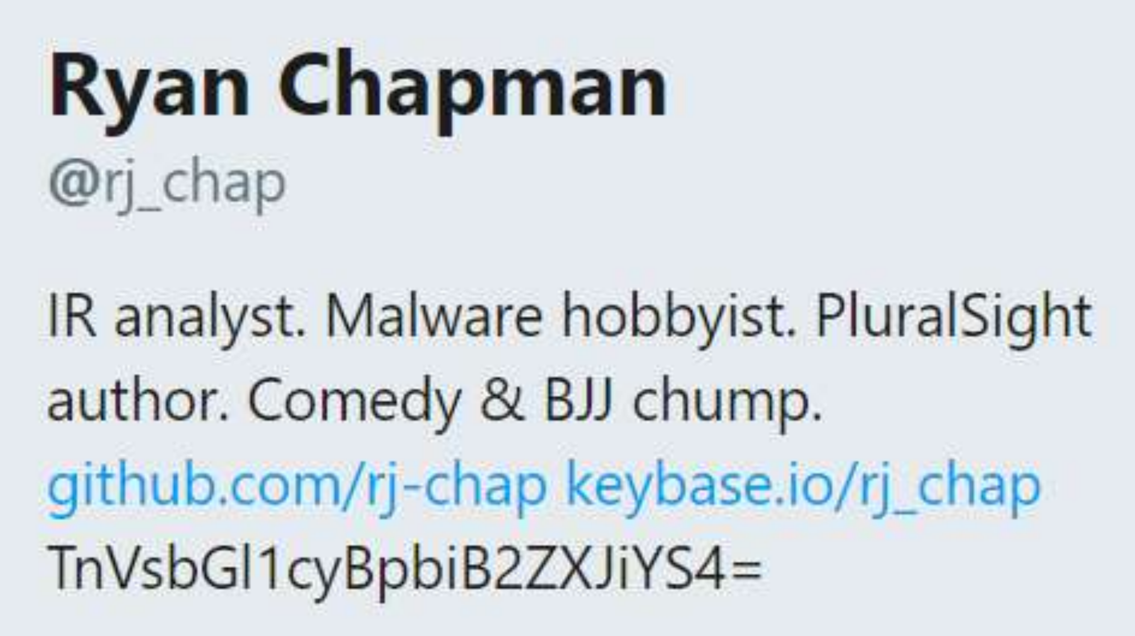
TABLETOPS

- Build muscle memory
- Optional or required?
- Time investment
    - Worth it!

QUIZZES

- Testing during or after
- Setup an LMS
    - Ex: Moodle
- Not as time intensive

QUESTIONS?



Ryan Chapman

@rj_chap

IR analyst. Malware hobbyist. PluralSight author. Comedy & BJJ chump.
github.com/rj-chap keybase.io/rj_chap
TnVsbGl1cyBpbiB2ZXJiYS4=