Pre-Lecture Activities

- There are ***no* pre-lecture review questions** for today
- But **you can**:
  - Ask questions about the **group project's** cases & instructions
  - Share **your team's preference** on the presentation week via Canvas

IFS4102: Digital Forensics

Lecture 8: Case Management, Forensic Analysis & Incident Response

Outline

- Forensic case management
- Case analysis
- Case reporting
- Case presentation

- Forensic analysis techniques
- Timeline analysis and tools

- Incident Response

Forensic Case Management

Case Management: FORZA Framework

- ***FORensics ZAchman framework (FORZA)*** framework:
  - A technology-independent digital forensics **investigation framework**
  - It binds **roles**, **responsibilities** & **procedures** together
- **Eight** separate roles & responsibilities (but some could be handled by the same person):
  - Case leader
  - System/business owner
  - Legal advisor
  - Security/system architect/auditor
  - **Digital forensics *specialist***: to plan the entire operations
  - **Digital forensics *investigator*/system administrator/operator**: to collect, extract, preserve and store the digital evidence
  - **Digital forensics *analyst***: to extract relevant data, analyze them
  - Legal prosecutor

Table 2 – A high-level view of the FORZA framework

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

FIGURE 6.4 High-level framework for FORZA model in Ieong (2006).

FORZA Framework

- Six categories of **concerns/questions** (5WH):
  - Why (motivation)
  - What (data attributes)
  - How (procedures/functions)
  - Where (location & network)
  - Who (people)
  - When (time)
- **Tasks** of each role/responsibility on each category are identified: *see the table*
- Reference: https://www.sciencedirect.com/science/article/pii/S1742287606000661

Forensics Expert Witness: Duty & Issues

- **Duty**: to present the *objective/unbiased* truth of the matter before the court
- Some **common issues** faced:
  - Resisting influences
  - Avoiding preconceived theories
  - Scientific truth vs **legal judgment**:
    scientific & technical evidence is **only part** of the total picture
    - Scientific truth are **subordinate** to legal judgment:
      the outcome may *not* conform to the scientific truth
    - Digital investigators must generally accept an **attorney's decision not to proceed** with a case or **not to disclose** certain evidence

Pre-Investigation *Considerations*

- Potential **conflict of interest**
- **Availability**: impact on other jobs & commitments
- **Location & environment**
- **Logistics**: travel/transport, accommodation, communications
- **Resources**
- Involved **parties**:
  - Investigation initiator/requestor
  - Who is paying the bill?? Have they got the loot?
  - Economics: is the cost worth the outcome (criminal or civil)?
- Post-case **actions**

Purpose **of the Investigation**

- What is the ***outcome*** sought?
  - Investigation
  - Intelligence
  - Just being a nuisance
- ***Type*** of investigation:
  - Covert or overt
  - Criminal, civil, family/matrimonial
- Your ***positioning***:
  - Which **side** are your on
  - **Independence** as an expert
- What type of ***output/report*** does the client want

Planning & Preparation: Some Tips

- Create a **plan**
  - And stick by it: your plans becomes a **checklist**
- **Prepare** for the job:
  - Knowledge
  - Equipment
  - Time: how long should you allow
  - Logistics: accommodation, meals, transport
  - Donor media
  - Support strategy
  - Environment: safety (physical, biological, psychological)
  - Court considerations

Case Analysis

Review

DF Investigation Goal: Crime Reconstruction

- **Crime (scene) reconstruction**:
  the process of determining **the most likely hypothesis**, or **sequence of events**, through the application of the **scientific method**
- **5WH** defines the objectives of an investigation as:
  Who, What, Where, When, Why, How
- Some **main aspects** of analysis:
  - **Temporal** (related to time)
  - **Relational** (relationships of people and objects)
  - **Functional** (conditions necessary for the crime to occur)
  - **Victimology** (victim's characteristics)
  - Crime scene **characteristics**

Levels of Certainty in Digital Forensics

- The need to estimate & describe the ***level of certainty***
- **Problem**: *no* formal mathematics/statistics to evaluate levels of certainty associated with digital evidence
- **Issues**:
  - A lack of **consistency** of how accuracy is assessed
  - **Complexity** and multiplicity of computer systems
  - Computers can introduce **errors & uncertainty**:
    e.g. incorrect system clock, spoofed/proxied IP address, etc.
  - Different knowledge & experience of the **investigators**
- An **informal system** of degrees of likelihood in both the affirmative & negative sense:
  - (1) almost definitely, (2) most probably, (3) probably, (4) very possibly, (5) possibly

The Certainty Scale

- **Goal**: to **formalize** the process by which digital investigators assign **a level of certainty** to conclusions

Table 3.1 A Proposed Scale for Categorizing Levels of Certainty in Digital Evidence

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts	Erroneous/incorrect
C1	Evidence is highly questionable	Highly uncertain
C2	Only one source of evidence is not protected against tampering	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g., temporal error and data loss)	Almost certain
C6	The evidence is tamperproof or has a high statistical confidence	Certain

Source: Casey, *Digital Evidence and Computer Crime*, 3rd Edition

Case Reporting

Forensic Report

- **Goal: to communicate/report** the results of your forensic investigation
- **Roles** of a report:
  - Presents evidence admissible in a **court of law**
  - As an **affidavit** to support issuing a search warrant or an arrest
  - Supports **further investigation**
  - Can be used by your organization for its **subsequent actions**
- **Written** report requirement
- *What should be **included** in your written report?*
  - The task assigned
  - A factual statement
  - Acquired evidence

Forensic Report

- The steps taken
- The equipment & methodologies used
- The facts or data that support or reject the statement
- Findings
- Conclusions

- Federal Rules of Civil Procedure (FRCP), Rule 26 on an **expert witness's written report content**:
  - All **opinions**, the basis for the opinions, information considered in coming to the opinions, related ***exhibits*** (photographs, diagrams)
  - **CV***

** Not required for your group-project reports*

Report *Outline*: By Melia Kelley

- **Title Page**: Case name, date, investigator name, contact information
- **Table of Contents**
- **Executive Summary:** High-level view of important findings
- **Objectives:** Brief case description and your investigation goals
- **Evidence Analyzed**:
  - Serial numbers, hash values, pictures taken at the scene, etc.
  - (**List, label and summarize** your pieces of evidence!)
- **Steps Taken**: Your results should be reproducible including the software & hardware used, version numbers
  - Also explain your data **collection & examination methods**, and state about your evidence **integrity**

Report *Outline*: By Melia Kelley

- **Relevant Findings**: Documents of interest; Internet activity; Software of note; USB Devices, etc.
- **Timeline:** A concise timeline of **important events**, possibly using a good graphic (*very important!)*
- **Other diagrams**: **Spatial diagram**, **entity & evidence relationship diagram**
- **Conclusion:** Highlight the important issues in a list of concise findings
- **Signature**: Your report should be signed
- **Exhibits**: Your CV, chain of custody documentation, supporting document linked from the body of the report, etc. (*see the next slide)*

Possible additional sections: **Glossary**, **References**, **Acknowledgement**

Reference:
http://www.forensicmag.com/article/2012/05/report-writing-guidelines

Exhibits

- ***Exhibits***: photos, diagrams, video/audio recordings, …
- *Why including exhibits*?
  written word cannot always explain things,
  so it's useful to use ***other types* of material**
- **As evidence**:
  - The items need to be introduced via a statement or affidavit as an **annexure**
  - As with all your evidence, an object is **open to challenge**
- In the **analysis process**:
  - You describe how an object was **created**
  - Explain how the cited exhibits **support** your conclusions

Notes on Your Analysis & Conclusions

- Your statements & conclusion should be stated in an **objective** and **accurate** way
- Some useful **phrases**:
  - "The evidence indicates/suggests…"
  - "It is my professional opinion that…"
  - "Based on my knowledge…"
- You can include **uncertainty & error analysis**:
  - **No absolute** assurance, hence it is important *not* to overreach
  - Include a statement of "**limitations of knowledge**" & **uncertainty**
  - E.g. **MAC times**: timestamp can be incorrect/reset/tampered/etc.
  - Yet, you can still compellingly argue your conclusions based on other **available reliable indicators**

Case Presentation

Presentation

- Probably the ***most* critical part** of computer forensics
- Most of our work is **geared** to a presentation to a court or an administrative tribunal
- ***Prepare your presentation well!***

Ethics for Expert Witness

- Mind your **witness demeanour**!
- Codes of ***professional conduct* or responsibility**
- Its **not** about you:
  - Answer the question as asked
  - Clarify if necessary, but do not dig a hole in the process
- When **questioning** & **being questioned**:
  - The old adage that "lawyers only ask questions they know the answer" does apply
  - When asked a question, you must think about **where they are going** and **potential traps**
- *For more?* Take IFS4101 (Legal Aspects of Information Security)

Questions for Preparing Your Testimony

- Have I understood the **trial process**
- What's **my story/opinion** of the case
- What's the **client's overall theory** of the case
- How does my opinion **fit** into the theory of the case
- What can I say **with confidence**, what can't
- What's the **scope** of the case w.r.t. my role in the case? Have I gone too far with my testimony?
- How can I **explain** my findings well including to **laymen**: have I prepared graphics and other supporting materials?
- Have I prepared **definitions of technical concepts** that I use when questioned

Forensic Analysis Techniques

General Forensics Analysis Steps

- General case-analysis **steps**:
  - Disk analysis
  - Partition/file-system analysis
  - Deleted file retrieval
  - Data carving for hidden data recovery
  - Various artefact analysis, including by using Autopsy modules
  - ***Timeline analysis***
  - ***Crime-reconstruction analysis***: to answer **5WH**

Crime-Reconstruction Analysis

- ***Temporal* analysis**:
  - **Timeline analysis** of **events** and their relevant objects/actors/…
  - Possible representations: tabular view, graph view/model
- ***Spatial* analysis**:
  - Geographical **locations** of actors, objects, communications, …
  - Map-based visualization
- ***Conceptual* analysis**:
  - **Entity & evidence *relational* analysis**:
    entity & evidence relationship diagram
  - …

Spatial Analysis

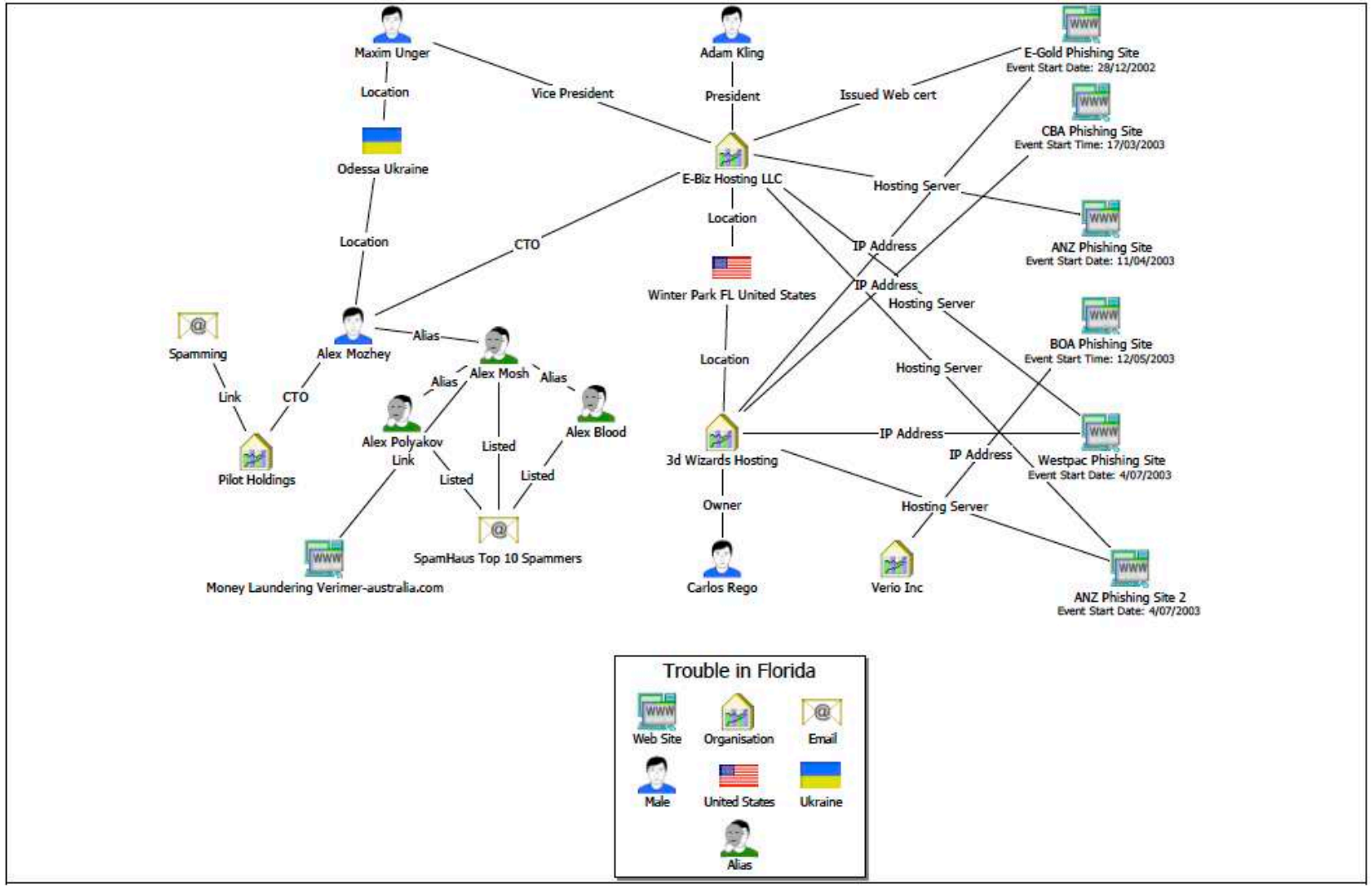
- **Spatial analysis**:
  shows **geographical locations** of actors, objects, communications, etc.
- A standard technique: ***map-based visualization***
  - An **example** is shown on the next slide

FIGURE 8.3 Offender in Europe, victim in the United States, crime scenes spread around the world on personal computers and servers (AOL in Virginia).

Conceptual Analysis: Relational Analysis

- **Entity & evidence relational analysis**: shows the **relationships** among all involved **entities**, **evidence**, and their properties
- A sample ***entity & evidence relationship diagram***: **a phishing attack** (*see the next slide*)
  - **Relationship** of phishing sites, hosting companies, and company officers
  - Link to possible **suspects**: country, known spammers, …
  - …

Relational Analysis: Example



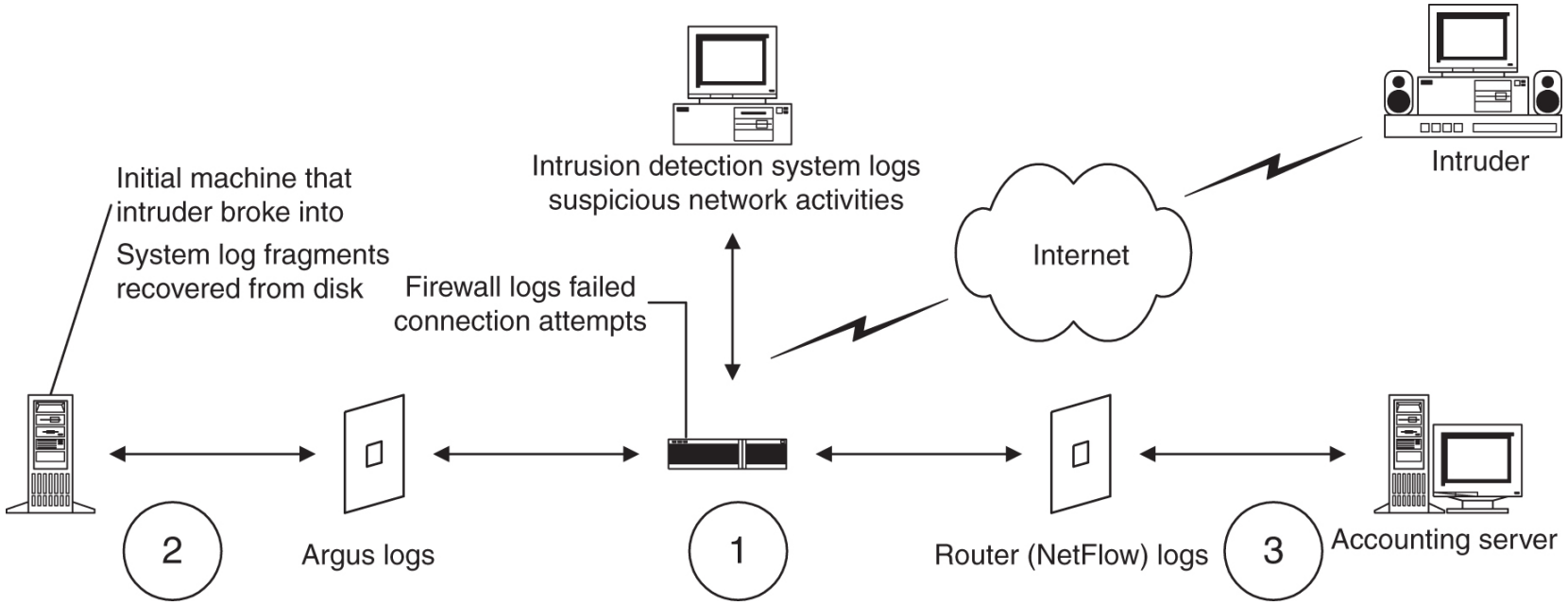


FIGURE 8.2 Diagram depicting intruder gaining access to accounting server.

Timeline Analysis

Timeline Analysis

- *How to **view & analyze** artefacts containing time information?*
- ***Timeline analysis***: useful in a wide variety of forensic cases:
  - When was this email written?
  - Are there traces of malicious activity at a given time?
  - Are there any traces of other activity while this file was downloaded?
  - Was a person using this system at a specific time (alibi)?
  - …

Timeline Analysis Representation

- **Tabular/list view**:
  - Good for listing ***simple*** **time-ordered items** during a time period
  - Examples:
    - Profiling a **sequence of actions** performed by a set of users
    - Sequencing a number of **process executions**
    - Listing **files created**
- **Graph models**:
  - Needed for highlighting **more *complex* correlations**, which require multiple tabs, queries, …
  - Examples:
    - Listing **all users** that were logged into a system that executed **a set of processes** in questions

NIST's Data Leakage Case: *Tabular View*

Detailed behavior of the suspect is described as a text (below table) and visual diagram.

Step	Date/Time	Action	Additional Description	Note
Normal	~ 2015-03-22	Install OS	Windows 7 Ultimate	
		Configure settings	Set the timezone to (UTC-05) Eastern Time	
		Install Apps	(1) Microsoft Office (2) Microsoft Internet Explorer (3) Google Chrome	Latest versions if possible
		Create/Download business data	Electronic documents (Word, Excel, PowerPoint...)	Company's common files
		Email	Microsoft Outlook with NIST e-mail account	iaman.informant@nist.gov
		Create user accounts	"admin11" → login count: 2 "ITechTeam" → login count: 0 "temporary" → login count: 1	
D-2	2015-03-23 13:29	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Hello, Iaman] "How are you doing?"
	2015-03-23 14:01 ~ 2015-03-23 14:21	Prepare a crime (data leakage)	Searching the leakage methods through web-browsers: - Microsoft Internet Explorer - Google Chrome	Google, Bing search engine ---------- Chrome 1) data leakage methods 2) leaking confidential information 3) information leakage cases 4) intellectual property theft 5) how to leak a secret ---------- IE 11 6) file sharing and tethering 7) DLP DRM 8) e-mail investigation 9) what is windows system artifacts 10) investigation on windows machine 11) windows event logs 12) cd burning method in Windows 13) external device and forensics ---------- Chrome 14) cloud storage 15) digital forensics 16) how to delete data 17) anti-forensics 18) system cleaner 19) how to recover data 20) data recovery tools
	2015-03-23 14:31	Connect USB	'RM#1' USB memory stick	
	2015-03-23 14:36	Search keywords	Searching confidential data using Windows Search function	Keyword: "secret"
	2015-03-23 14:37	Open files	[secret_project]_proposal.docx [secret_project]_design_concept.ppt	Open and read files
	2015-03-23 14:39	Copy & open files	Copying confidential files from 'RM#1' to 'PC'	"\Desktop\S data"
		[RM#1] RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt	[PC] %UserProfile%\Desktop\S data\[secret_project]_proposal.docx %UserProfile%\Desktop\S data\[secret_project]_design_concept.ppt	
	2015-03-23 14:39	Disconnect USB	Ejecting 'RM#1'	
	2015-03-23 14:39	Configure settings	Show 'file name extensions' in Windows Explorer	
	2015-03-23 14:41	Rename files	All names and extensions are changed (e.g., xlsx → jpg, docx → mp3...)	[secret_project]_detailed_proposal.docx → landscape.png [secret_project]_design_concept.ppt → space_and_earth.mp4

From: NIST, *NIST CFReDS: Data Leakage Case*, July 2018

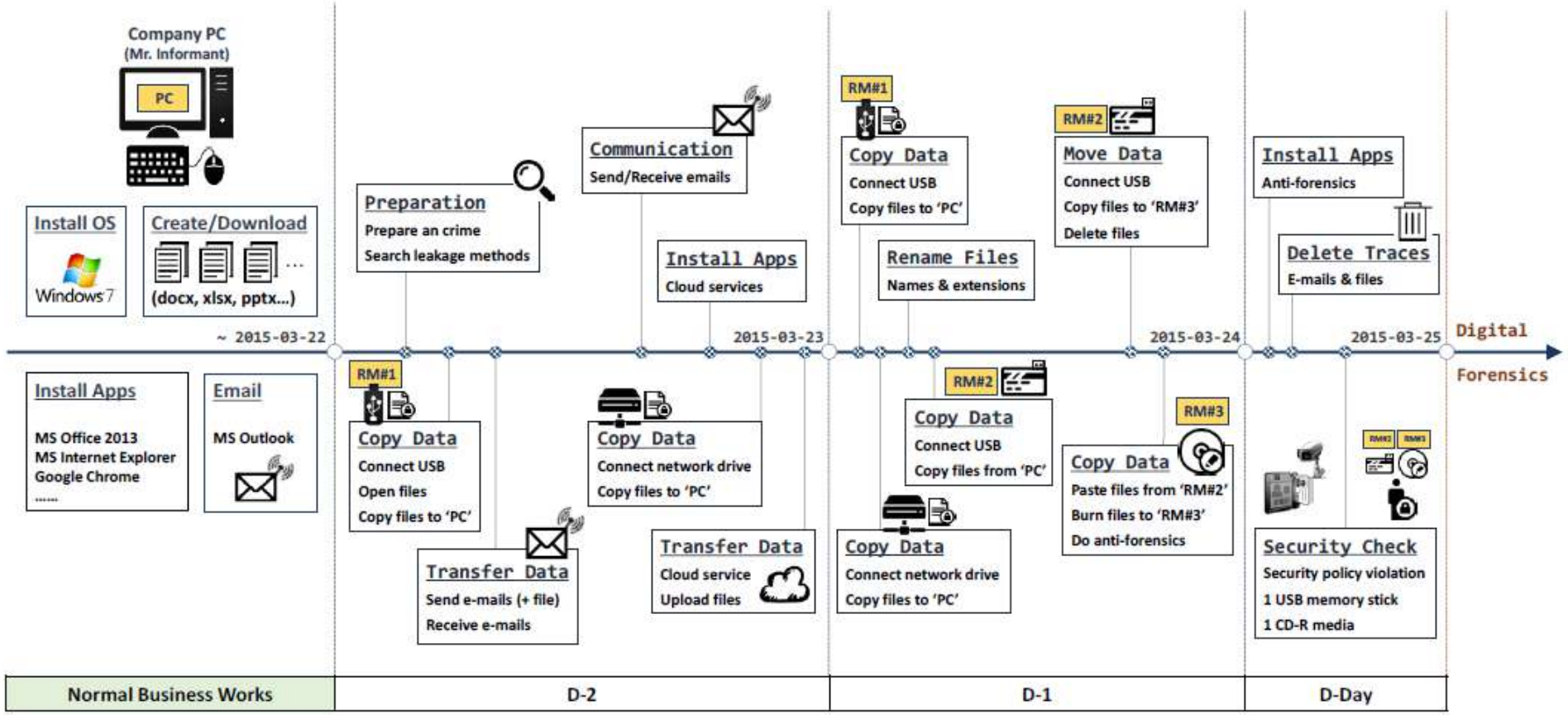
NIST's Data Leakage Case: *Tabular View*

	2015-03-24 16:54	Copy files	Copying and burning confidential files from 'RM#2' to CD-R	
	2015-03-24 16:55	Rename directories	Renaming directories in CD-R	
	2015-03-24 16:57	Copy files	Copying 3 meaningless files to CD-R	Koala.jpg Penguins.jpg Tulips.jpg
	2015-03-24 16:58	Delete files	Deleting confidential files from CD-R	
	2015-03-24 17:01	Verify files	Traversing directories and files in CD-R using Windows Explorer	
	2015-03-24 17:02	Delete files	Deleting copied files from 'RM#2' (Quick format)	Anti-forensics
	2015-03-24 17:03	Disconnect USB	Ejecting 'RM#2'	
	2015-03-24 17:05	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	[Subject: Done] "It's done. See you tomorrow."
	2015-03-24 17:06	Search keywords	Searching keywords using Chrome	"security checkpoint CD-R"
D-Day	2015-03-25 10:46	Search and download Apps	Searching apps for anti-forensics using IE	Anti-forensic tools, eraser, ccleaner…
	2015-03-25 10:50	Install Apps	(1) Eraser (with .NET Framework) (2) CCleaner	During approx. 8 minutes
	2015-03-25 11:00	Delete e-mails	Deleting some e-mails in Outlook	Anti-forensics (9 emails are deleted, and 4 items of them remain in Deleted Items folder.) During approx. 10 minutes
	2015-03-25 11:13	Delete traces	Running anti-forensic tools and deleting some files	Wiping "\Desktop\temp" directory using Eraser
	2015-03-25 11:14	Delete traces	Emptying the Recycle Bin	
	2015-03-25 11:15	Delete traces	Deleting downloaded installer files (Eraser, CCleaner)	Normal deletion: [Shift] + [Delete]
	2015-03-25 11:15	Delete traces	Launching CCleaner	And then, the app was closed after doing nothing
	2015-03-25 11:18	Delete Apps	Uninstalling some Apps	CCleaner, iCloud During approx. 2 minutes
	2015-03-25 11:22	Delete traces	Launching Google Drive app and disconnecting an account	Logout from Google Drive
	2015-03-25 11:23	Delete traces	Cleaning and arranging Windows desktop	Directories and icons in Windows Desktop
	2015-03-25 11:24	Open files	Opening the resignation letter (.docx)	Windows Desktop
	2015-03-25 11:28	Print files	Printing the document to the MS XPS file and reviewing it with MS XPS viewer	
	2015-03-25 11:30	Finish works	Turning off the system and trying to go outside with 'RM#2' and 'RM#3'	RM#3 is one of two CD-Rs

From: NIST, *NIST CFReDS: Data Leakage Case*, July 2018

NIST's Data Leakage Case: *Graphical* Timeline Diagram

Graphical Timeline of the Data Leakage Scenario



From: NIST, *NIST CFReDS: Data Leakage Case*, July 2018

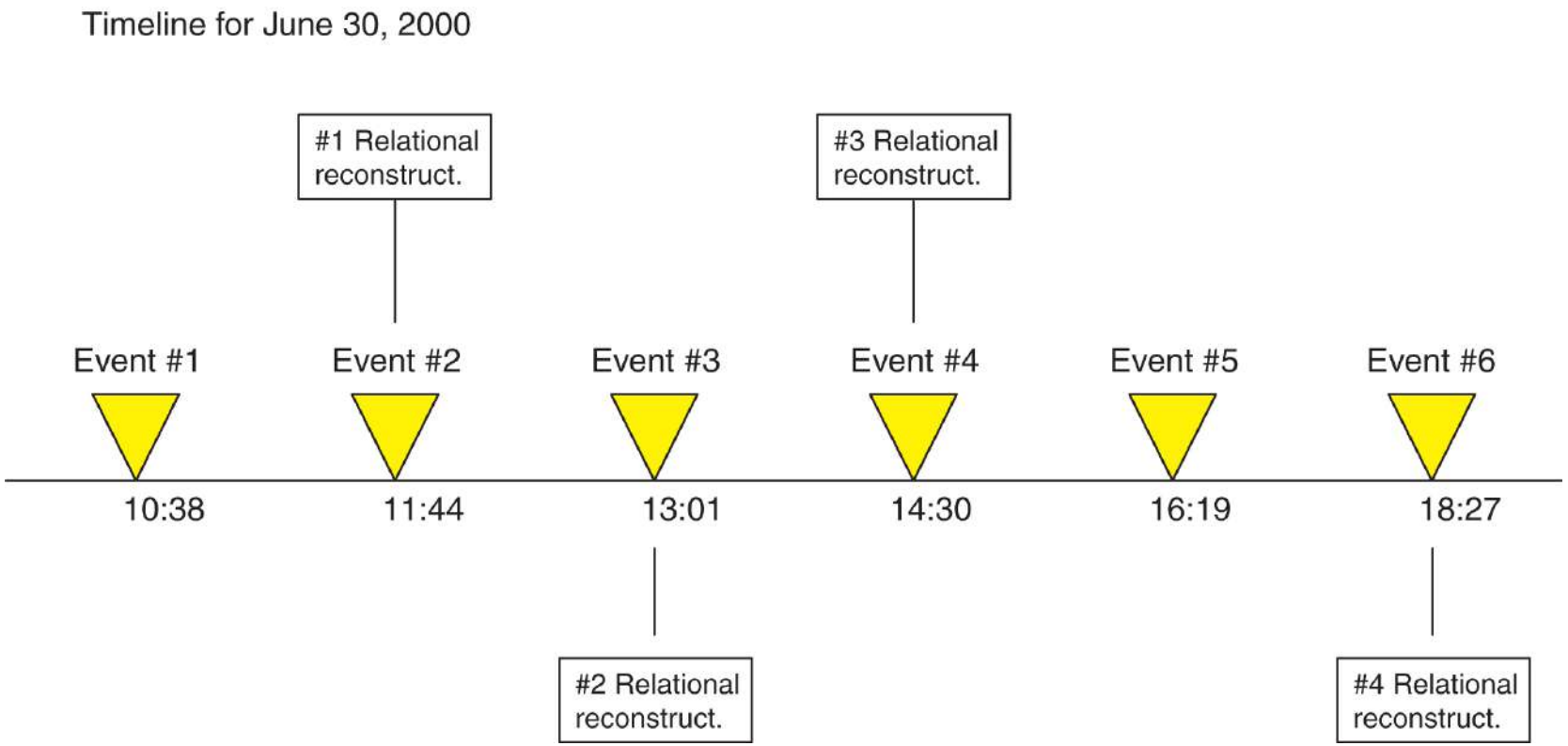
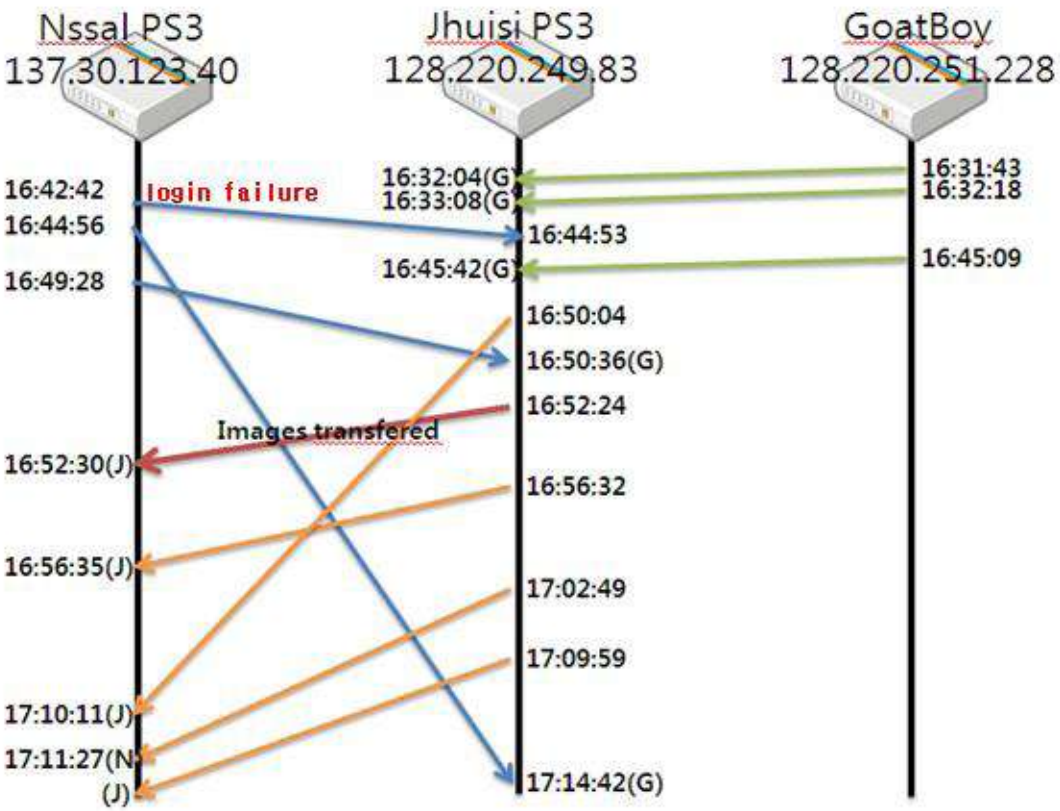


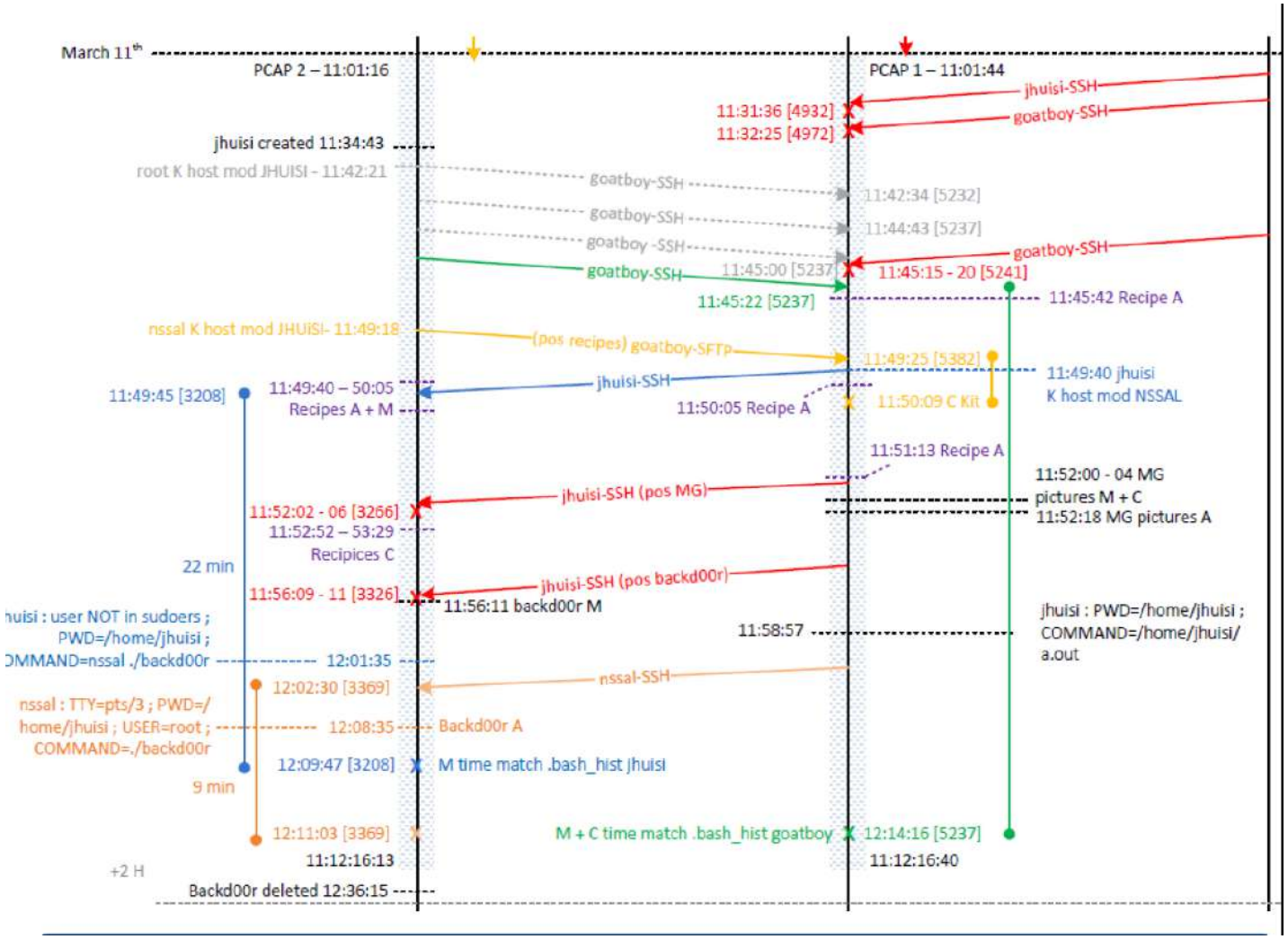
FIGURE 8.1 Conceptual view of timeline and relational reconstructions.

Timeline Analysis: Graph Model - Communication Events



Digital Forensics Research Workshop Challenge 2009

Timeline Analysis: Graph Model - Communications & File Accesses

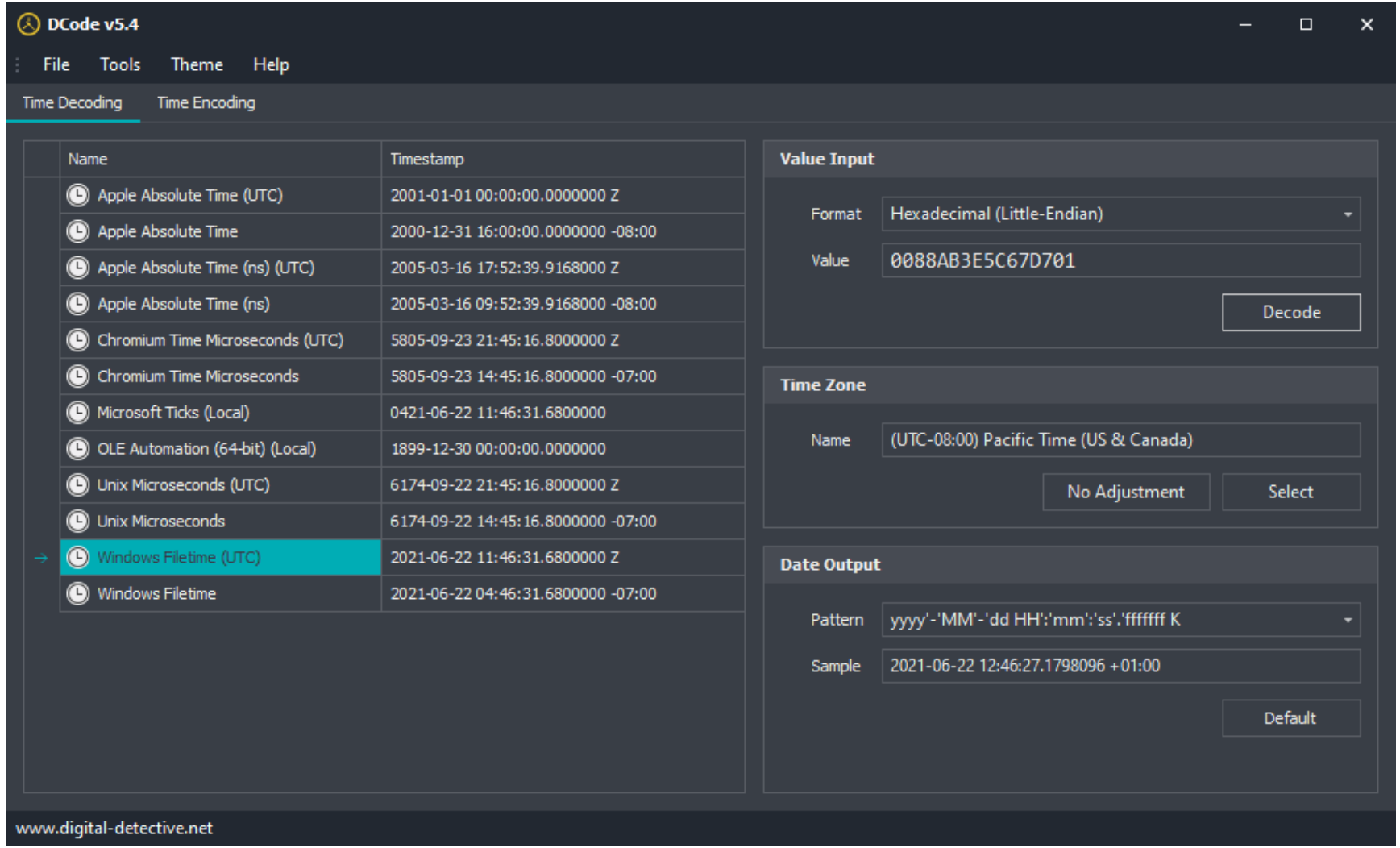


Digital Forensics Research Workshop Challenge 2009

Some Useful Time-Analysis *Tools*

- **DCode**: for time format conversion
- The TSK's **mactime**: http://wiki.sleuthkit.org/index.php?title=Mactime
- **Autopsy's Plaso & Timeline**: *see Task 1 of Lab 8*
- **Log2timeline/Plaso**: *see (optional) Task 2 of Lab 8*
  - https://github.com/log2timeline/plaso
  - https://plaso.readthedocs.io/en/latest/
  - https://www.youtube.com/watch?v=sAvyRwOmE10 (*very good!*)
- **Timeline Explorer**: *see (optional) Task 2 of Lab 8*

DCode



From: https://www.digital-detective.net/dcode/)

TSK's mactime

- **mactime**:
  - A useful **TSK's tool** to create an ASCII **timeline of file activity**
- First, a ***body file*** can be generated by fls or ils:
  - `fls -f ext3 -m "/" -r` <*disk-image-file*> `> body-file.txt`
  - `ils -f ext3 -m` <*disk-image-file*> `>> body-file.txt`
- The body file contains a line for each file or event
- Next, mactime takes the body file as input and **sorts the data** based on its temporal data:
  `mactime -b body-file.txt > timeline-file.txt`
- There are some other options:
  see https://wiki.sleuthkit.org/index.php?title=Mactime

Log2timeline/Plaso

- **Goal**: Collect all timestamped events of interest, and aggregate them in a single place for a ***super timeline* analysis**
- ***Super timeline***: a timeline of timelines that are gathered from the *file system*, *registry keys*, and *other artifacts*, which produces **a single correlated timeline**
- **Log2timeline**: a tool designed to extract **timestamps** from various files, and aggregate them
- **Plaso**:
  - A Python-based **backend engine** for log2timeline
  - Has become a **framework** that supports, among others: new parsers or parsing plug-ins, analysis plug-ins, etc.

Log2timeline/Plaso: Kali Linux

GET KALI BLOG DOCUMENTATION COMMUNITY COURSES DEVELOPERS ABOUT

Packages and Binaries:

plaso

This is a metapackage that depends on the Python 3 package of the Plaso libraries and scripts.

Installed size: `40 KB`
How to install: `sudo apt install plaso`

```
root@kali:~# log2timeline.py -h
usage: log2timeline.py [-h] [--troubles] [-V] [--artifact_definitions PATH]
                       [--custom_artifact_definitions PATH] [--data PATH]
                       [--artifact_filters ARTIFACT_FILTERS]
                       [--artifact_filters_file PATH] [--preferred_year YEAR]
                       [--process_archives] [--skip_compressed_streams]
                       [-f FILE_FILTER] [--hasher_file_size_limit SIZE]
                       [--hashers HASHER_LIST]
                       [--parsers PARSER_FILTER_EXPRESSION]
                       [--yara_rules PATH] [--partitions PARTITIONS]
                       [--volumes VOLUMES] [--language LANGUAGE_TAG]
                       [--no_extract_winevt_resources] [-z TIME_ZONE]
                       [--no_vss] [--vss_only] [--vss_stores VSS_STORES]
                       [--credential TYPE:DATA] [-d] [-q] [-u] [--info]
                       [--use_markdown] [--no_dependencies_check]
                       [--logfile FILENAME] [--status_view TYPE] [-t TEXT]
                       [--buffer_size BUFFER_SIZE] [--queue_size QUEUE_SIZE]
                       [--single_process] [--process_memory_limit SIZE]
                       [--temporary_directory DIRECTORY] [--vfs_back_end TYPE]
                       [--worker_memory_limit SIZE] [--worker_timeout MINUTES]
                       [--workers WORKERS] [--sigsegv_handler]
                       [--profilers PROFILERS_LIST]
                       [--profiling_directory DIRECTORY]
                       [--profiling_sample_rate SAMPLE_RATE]
                       [--storage_file PATH] [--storage_format FORMAT]
                       [--task_storage_format FORMAT]
                       [SOURCE]
```

Source: https://www.kali.org/tools/plaso/

log2timeline.py

- Extracts events from individual **files**, recursing a **directory** (e.g. mount point), **disk image file**, or **device**
- Creates an SQLite-based ***"Plaso storage"*** **file** for analysis by pinfo & psort
- Sample output (see Lab 8):

```
plaso - log2timeline version 20200121

Source path             : /home/sansforensics/EventLogs
Source type             : directory
Processing time         : 00:00:21

Tasks:          Queued  Processing      Merging         Abandoned       Total
                0       0               0               0               3

Identifier      PID     Status          Memory          Sources         Events          File
Main            2940    completed       148.3 MiB       3 (0)           19762 (0)
Worker_00       2947    idle            115.4 MiB       0 (0)           11137 (0)       OS:/home/sansforensics/EventLogs/System.evtx
Worker_01       2949    idle            116.4 MiB       2 (0)           8625 (0)        OS:/home/sansforensics/EventLogs/Security.evtx

Processing completed.

Number of warnings generated while extracting events: 214.

Use pinfo to inspect warnings in more detail.
```

pinfo & psort

- **pinfo**: provides **information** about the content of a storage file
- **psort**: post-processes (e.g. filter, sort, run automatic analysis) on the contents of a Plaso storage file
- **psteal**: a "*shortcut*" command that **combines** log2timeline & psort

```
plaso - psort version 20200121

Storage file            : events.plaso
Processing time         : 00:00:16

Events:         Filtered        In time slice   Duplicates      MACB grouped    Total
                0               0               0               19762           19762

Identifier              PID     Status          Memory          Events          Tags            Reports
Main                    3010    exporting       84.0 MiB        19762 (276)     0 (0)           0 (0)

Processing completed.
```

Log2timeline/Plaso: Sample Usage

```
root@siftworkstation:~# mmls /media/winXPSP2-w32Morto/diskimage.img
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000000   0000000062   0000000063   Unallocated
02:  00:00   0000000063   0312560639   0312560577   NTFS (0x07)
03:  -----   0312560640   0312581807   0000021168   Unallocated

root@siftworkstation:~# mount -t ntfs -o ro,loop,show_sys_files,streams_interface=windows,offset=32256 /media/winXPSP2-w32Morto/diskimage.img /
mnt/windows_mount/

root@siftworkstation:~# log2timeline.py -p  -z Europe/Rome  /media/winXPSP2-w32Morto/intrusion.plaso  /mnt/windows_mount/

root@siftworkstation:~# psort.py  -o list

******************************** Output Modules ********************************
 L2tcsv : The CSV format used by log2timeline, with 17 fixed fields.
 Dynamic : Dynamic selection of fields for a separated value output format.
 Rawpy : Prints out a "raw" interpretation of the EventObject.
 Raw : Prints out a "raw" interpretation of the EventObject protobuf.
 Sql4n6 : Saves the data in a SQLite database, used by the tool 4n6Time.
 Pstorage : Dumps event objects to a plaso storage file.
-------------------------------------------------------------------------------

root@siftworkstation:~# psort.py -z Europe/Rome intrusion-plaso.dump -o L2tcsv -w intrusion-plaso.csv

root@siftworkstation:~# l2t_process -b intrusion-plaso.csv 08-04-2014 > intrusion-plaso-filter.csv
```

1 Find the starting sector of the NTFS partition using mmls

2 Mount the NTFS partition in read only mode into / mnt/windows_mount

Offset is calculated by multiplying the start sector with unit per sector

63 x 512 = 32256

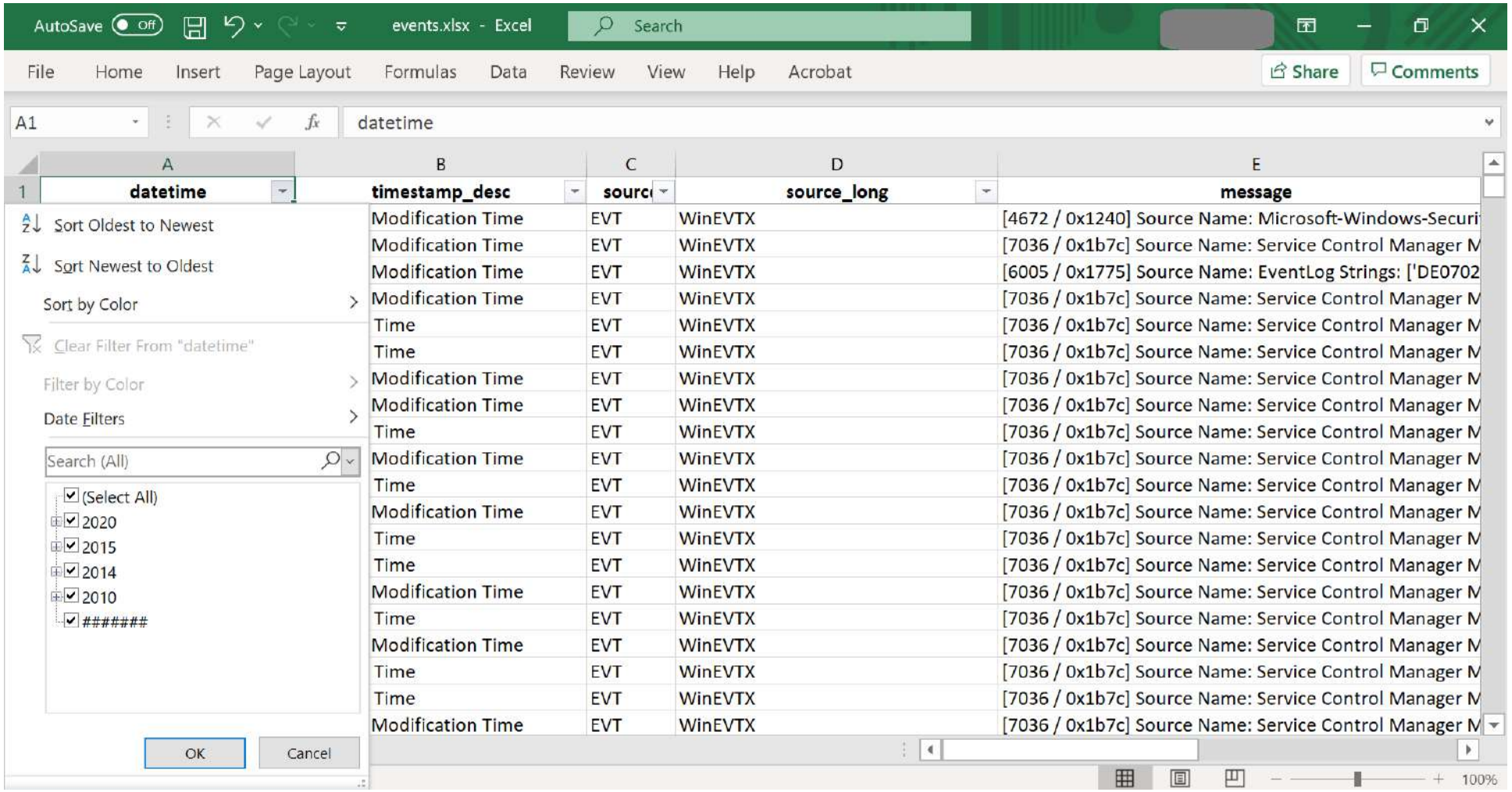
3 Process the mounted partition with all plugins and create the super timeline in plaso storage format

4 Sort the plaso file and generate super timeline output into CSV format

5 Reduce the data set to a date proximal to the intrusion

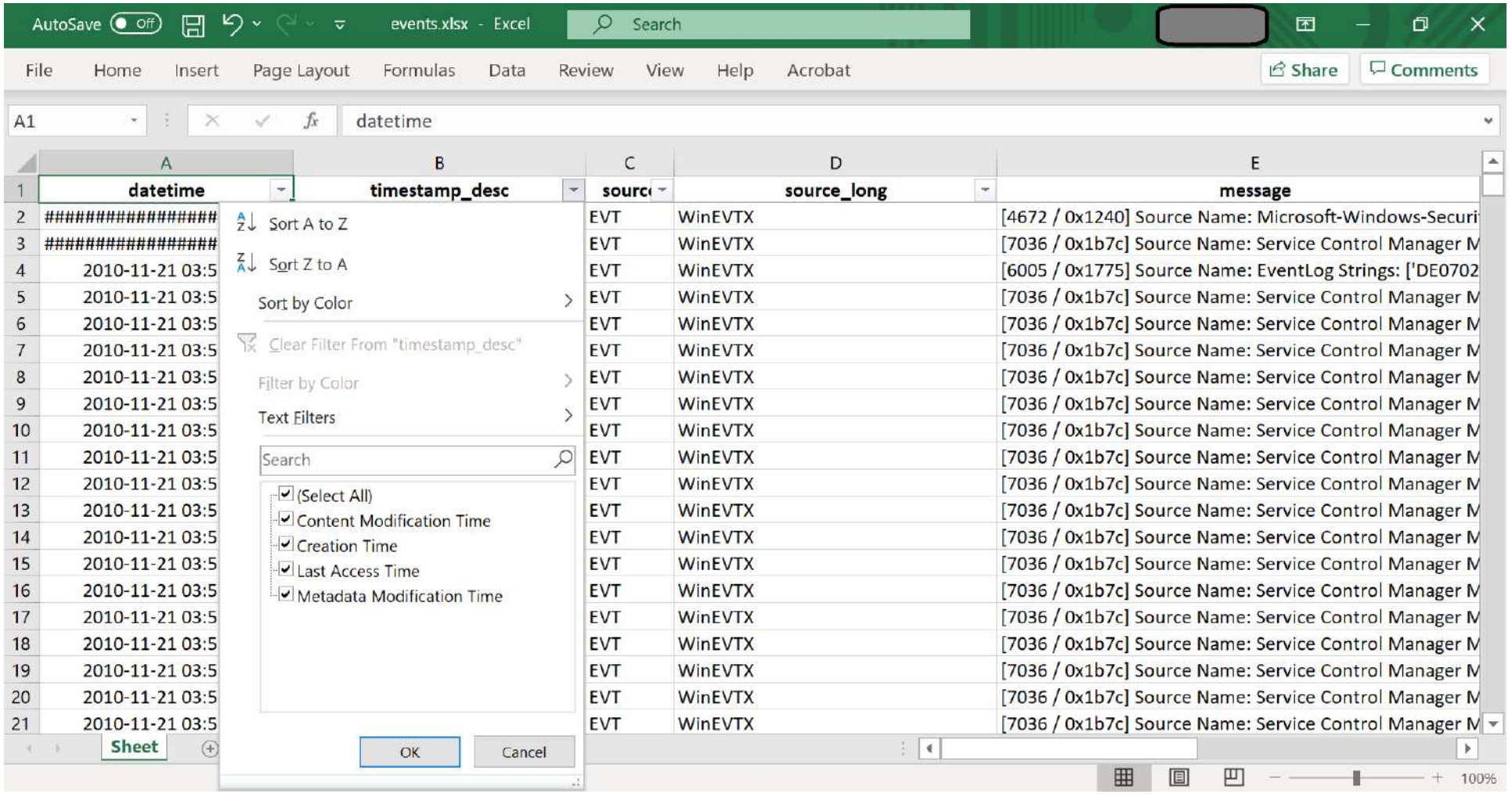
Source: https://countuponsecurity.com/2014/08/25/forensics-evidence-processing-super-timeline/

Log2timeline/Plaso: Sample Output (Lab 8)



datetime	timestamp_desc	source	source_long	message
	Modification Time	EVT	WinEVTX	[4672 / 0x1240] Source Name: Microsoft-Windows-Securi
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[6005 / 0x1775] Source Name: EventLog Strings: ['DE0702
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
	Modification Time	EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M

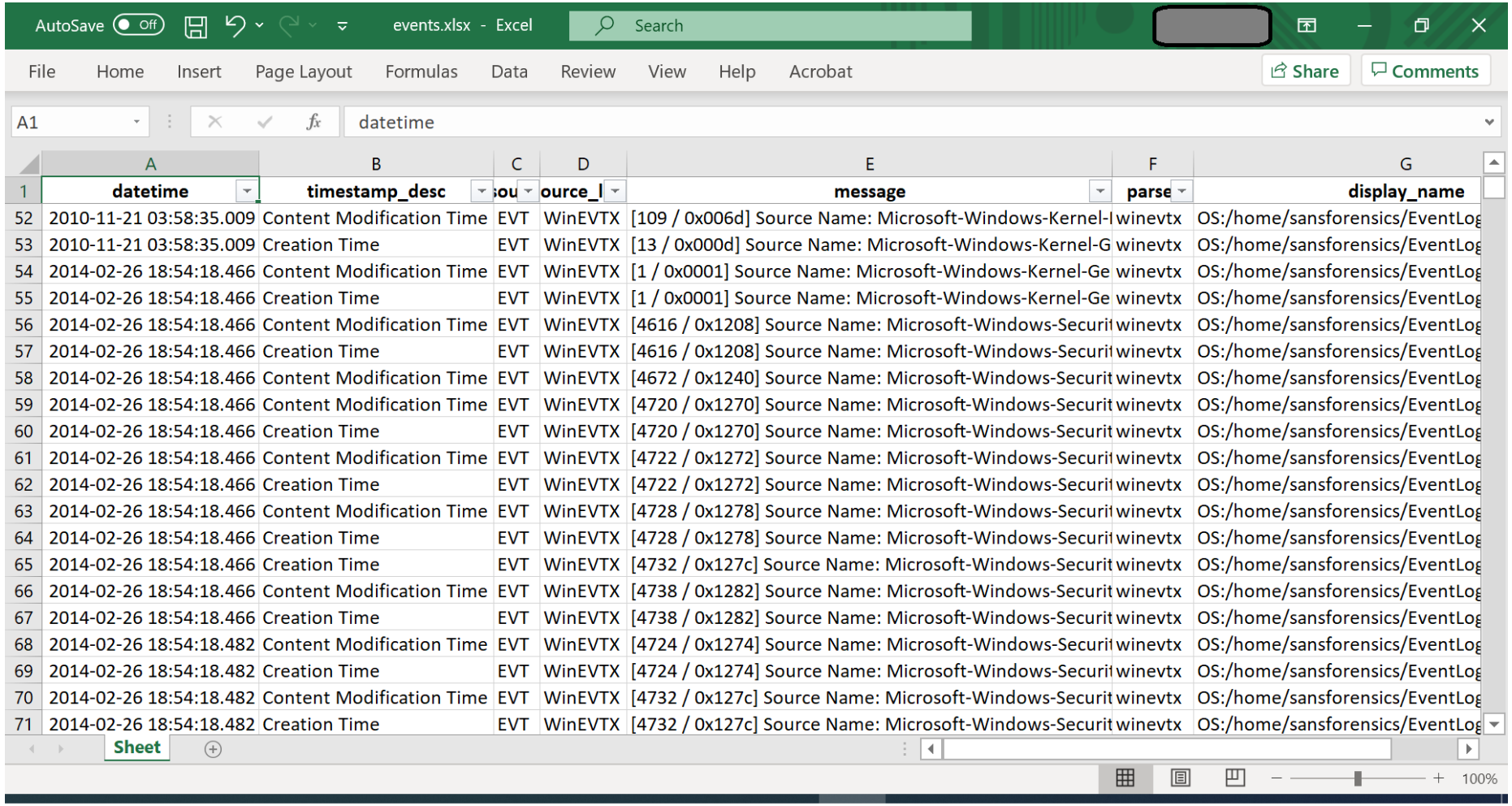
Log2timeline/Plaso: Sample Output (Lab 8)



☑ (Select All)
☑ Content Modification Time
☑ Creation Time
☑ Last Access Time
☑ Metadata Modification Time

	A	B	C	D	E
1	datetime	timestamp_desc	sourc	source_long	message
2	##################		EVT	WinEVTX	[4672 / 0x1240] Source Name: Microsoft-Windows-Securi
3	##################		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
4	2010-11-21 03:5		EVT	WinEVTX	[6005 / 0x1775] Source Name: EventLog Strings: ['DE0702
5	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
6	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
7	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
8	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
9	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
10	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
11	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
12	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
13	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
14	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
15	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
16	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
17	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
18	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
19	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
20	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M
21	2010-11-21 03:5		EVT	WinEVTX	[7036 / 0x1b7c] Source Name: Service Control Manager M

Log2timeline/Plaso: Sample Output (Lab 8)



	datetime	timestamp_desc	sou	ource_l	message	parse	display_name
52	2010-11-21 03:58:35.009	Content Modification Time	EVT	WinEVTX	[109 / 0x006d] Source Name: Microsoft-Windows-Kernel-I	winevtx	OS:/home/sansforensics/EventLog
53	2010-11-21 03:58:35.009	Creation Time	EVT	WinEVTX	[13 / 0x000d] Source Name: Microsoft-Windows-Kernel-G	winevtx	OS:/home/sansforensics/EventLog
54	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[1 / 0x0001] Source Name: Microsoft-Windows-Kernel-Ge	winevtx	OS:/home/sansforensics/EventLog
55	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[1 / 0x0001] Source Name: Microsoft-Windows-Kernel-Ge	winevtx	OS:/home/sansforensics/EventLog
56	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4616 / 0x1208] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
57	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4616 / 0x1208] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
58	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4672 / 0x1240] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
59	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4720 / 0x1270] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
60	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4720 / 0x1270] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
61	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4722 / 0x1272] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
62	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4722 / 0x1272] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
63	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4728 / 0x1278] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
64	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4728 / 0x1278] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
65	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4732 / 0x127c] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
66	2014-02-26 18:54:18.466	Content Modification Time	EVT	WinEVTX	[4738 / 0x1282] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
67	2014-02-26 18:54:18.466	Creation Time	EVT	WinEVTX	[4738 / 0x1282] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
68	2014-02-26 18:54:18.482	Content Modification Time	EVT	WinEVTX	[4724 / 0x1274] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
69	2014-02-26 18:54:18.482	Creation Time	EVT	WinEVTX	[4724 / 0x1274] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
70	2014-02-26 18:54:18.482	Content Modification Time	EVT	WinEVTX	[4732 / 0x127c] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog
71	2014-02-26 18:54:18.482	Creation Time	EVT	WinEVTX	[4732 / 0x127c] Source Name: Microsoft-Windows-Securit	winevtx	OS:/home/sansforensics/EventLog

More with Log2timeline/Plaso

- You can select the ***artefact types*** to be processed by specifying selected **parsers** with **`--parsers`** option
- Various different **parsers** are available, e.g.:
  - bash : Bash history files
  - chrome_cache : Chrome cache files
  - filestat : file system stat information
  - lnk: Windows Shortcut (LNK) files
  - prefetch: Windows Prefetch files
  - syslog : Syslog
  - winevt : Windows EventLog (EVT) files
  - winevtx : Windows XML EventLog (EVTX) files
  - …
- See: https://plaso.readthedocs.io/en/latest/sources/user/Parsers-and-plugins.html

Log2timeline/Plaso

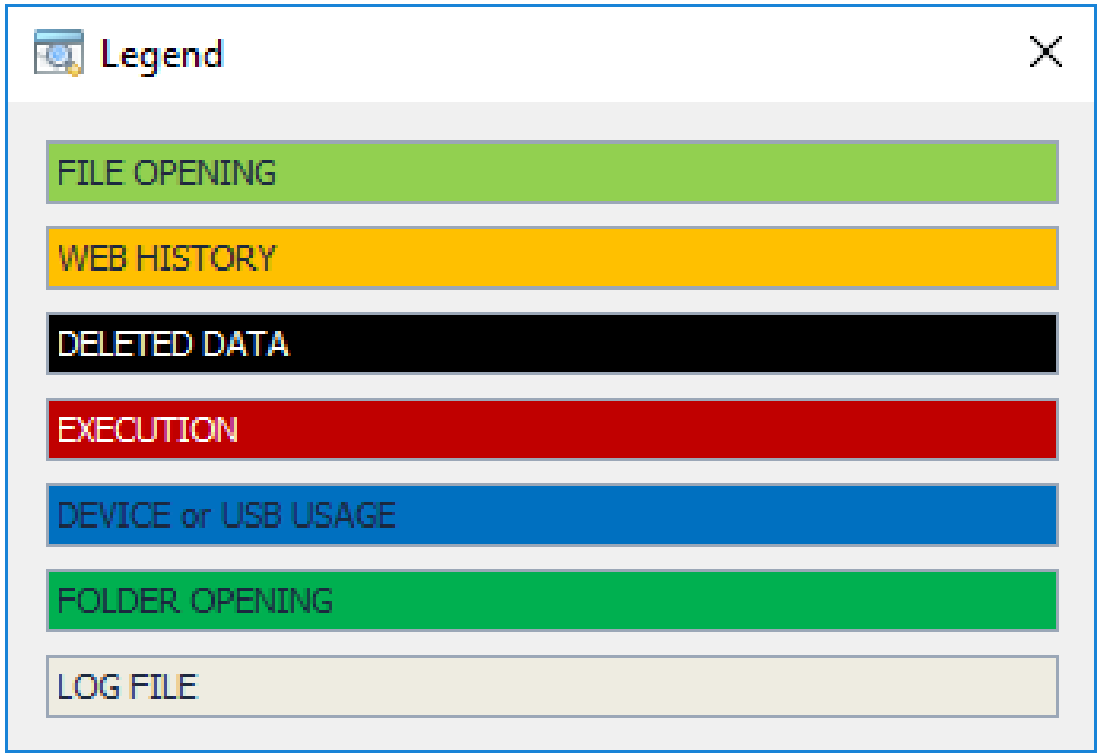
Available **references**:

- **Project** webpage: https://github.com/log2timeline/plaso
- **Documentation**: https://plaso.readthedocs.io/en/latest/
- **Installation**: https://plaso.readthedocs.io/en/latest/sources/user/Users-Guide.html#installing-the-packaged-release
- **Usage**: https://medium.com/@cloudyforensics/log2timeline-tutorial-d769994c3570, https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline/
- A **video** demo: https://www.youtube.com/watch?v=sAvyRwOmE10

Timeline Explorer

- A free, feature-rich ***Excel replacement*** that's catered specifically for **digital forensic examinations**
- Some useful **features**:
  - **Color coding** of events
  - Event-entry **grouping**, **searching**, **filtering** and **tagging**
- References:
  - https://aboutdfir.com/toolsandartifacts/windows/timeline-explorer/
  - https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html
- Videos:
  - https://www.youtube.com/watch?v=sAvyRwOmE10
  - https://www.youtube.com/watch?v=Hy8ZIc86tCo

Timeline Explorer: Color-Coding Feature



From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Timeline Explorer: Color-Coding Feature

Windows81_Windows2012R2_SYSTEM_AppCompatCache.tsv | supertimeline.csv | nromanoff-mactime-timeline-final.csv

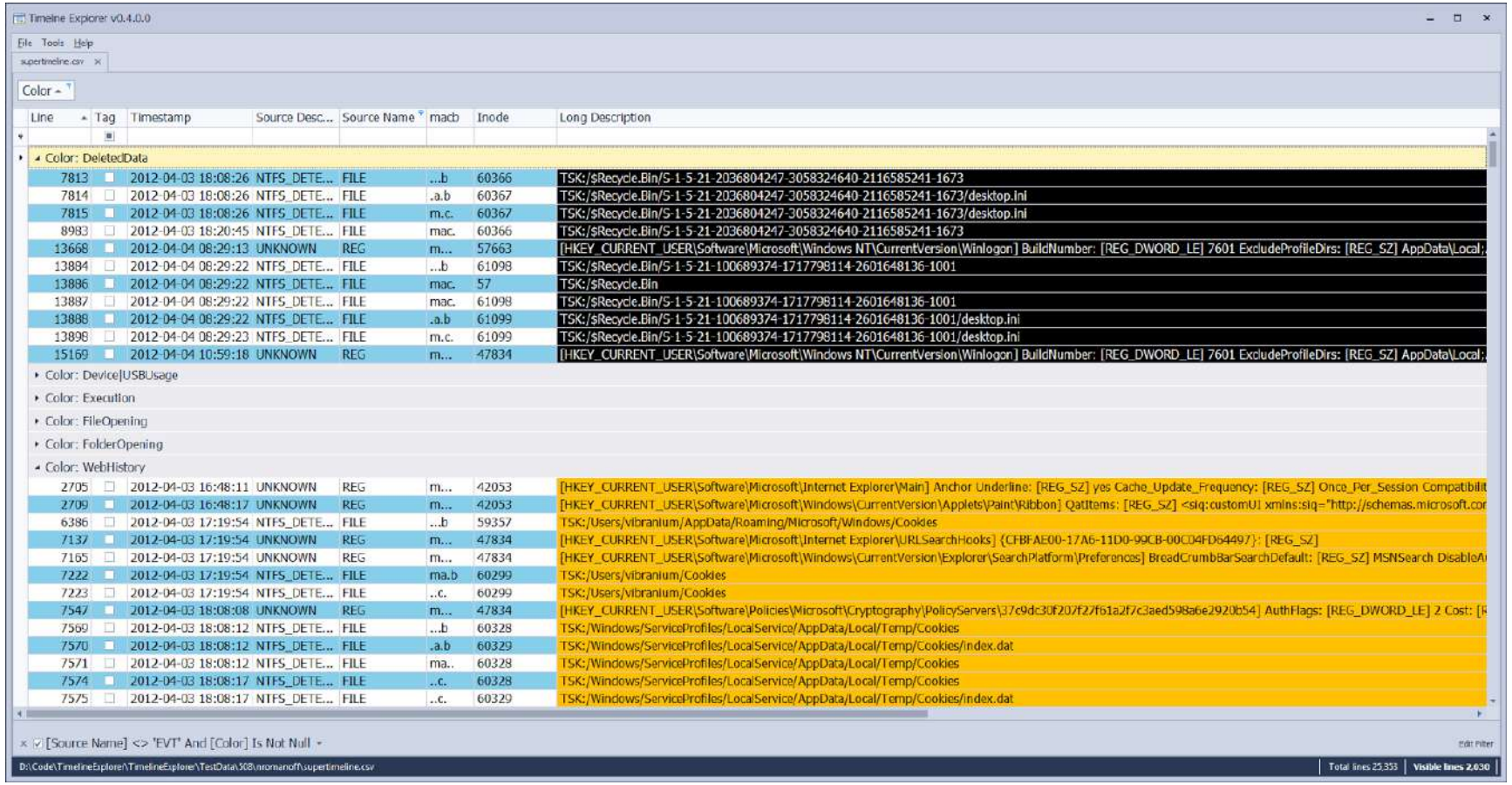
Drag a column header here to group by that column

Line	Tag	Timestamp	macb	Meta	File Name
16		2012-04-03 12:58:11	m.c.	16430-128-4	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report.html
17		2012-04-03 12:58:11	mac.	330-144-6	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics
18		2012-04-03 12:58:11	m.c.	47900-128-4	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-latest.xml
19		2012-04-03 12:58:11	macb	60199-128-1	C:/ProgramData/Microsoft/Windows/Power Efficiency Diagnostics/energy-report-2012-04-03.xml
20		2012-04-03 17:08:53	m...	42857-128-1	C:/Users/nromanoff/AppData/LocalLow/Microsoft/CryptnetUrlCache/MetaData/F063BF7EF604434CBE00FF1
21		2012-04-03 18:08:50	macb	0	[SHIMCACHE] \??\C:\$Recycle.Bin\S-1-5-21-2036804247-3058324640-2116585241-1673\$RR3GW21.exe
22		2012-04-03 18:08:50	macb	0	[SHIMCACHE] \??\C:\dllhost.exe
23		2012-04-03 18:08:50	macb	0	[SHIMCACHE] \??\C:\dllhot.exe
24		2012-04-03 18:33:16	.acb	0	[IEHISTORY] explorer.exe->:2012040320120404: vibranium@:Host: www.msn.com PID: 296/Cache type
25		2012-04-03 18:33:16	.acb	0	[IEHISTORY] explorer.exe->:2012040320120404: vibranium@http://www.msn.com/?ocid=iehp PID: 296
26		2012-04-03 20:25:31	.a.b	60240-128-4	C:/Windows/Prefetch/ATBROKER.EXE-FF58B71D.pf
27		2012-04-03 20:25:36	.a.b	60241-128-4	C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.41.g
28		2012-04-03 20:25:36	.a.b	60242-128-4	C:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.41.C
29		2012-04-03 20:25:38	.a.b	60244-128-4	C:/Windows/Prefetch/USERINIT.EXE-F39AB672.pf
30		2012-04-03 20:25:38	.a.b	60245-128-4	C:/Windows/Prefetch/DWM.EXE-AEABE78B.pf
31		2012-04-03 20:25:40	.a.b	60250-128-4	C:/Windows/Prefetch/VMWARETRAY.EXE-1DBB7768.pf
32		2012-04-03 20:25:40	.a.b	60251-128-4	C:/Windows/Prefetch/VMWAREUSER.EXE-83D1845B.pf
33		2012-04-03 20:26:18	macb	0	[Handle (Key)] MACHINE\SAM\SAM\DOMAINS\BUILTIN lsass.exe PID: 592/PPID: 464/POffset: 0x7dd796
34		2012-04-03 20:26:18	.a.b	60252-128-4	C:/Windows/Prefetch/NETPLWIZ.EXE-23BBB05C.pf
35		2012-04-03 20:26:42	.a.b	43048-128-4	C:/Windows/Prefetch/GPSCRIPT.EXE-9E16401F.pf
36		2012-04-03 20:38:07	mac.	2571-144-1	C:/Windows/System32/GroupPolicy
37		2012-04-03 20:38:07	...b	394-144-1	C:/Windows/System32/GroupPolicy/Machine
38		2012-04-03 20:38:07	m.c.	58169-128-1	C:/Windows/System32/GroupPolicy/gpt.ini
39		2012-04-03 20:38:13	mac.	394-144-1	C:/Windows/System32/GroupPolicy/Machine

D:\Code\TimelineExplorer\TimelineExplorer\TestData\508\nromanoff\nromanoff-mactime-timeline-final.csv | Total lines 8,146 | Visible lines 8,146

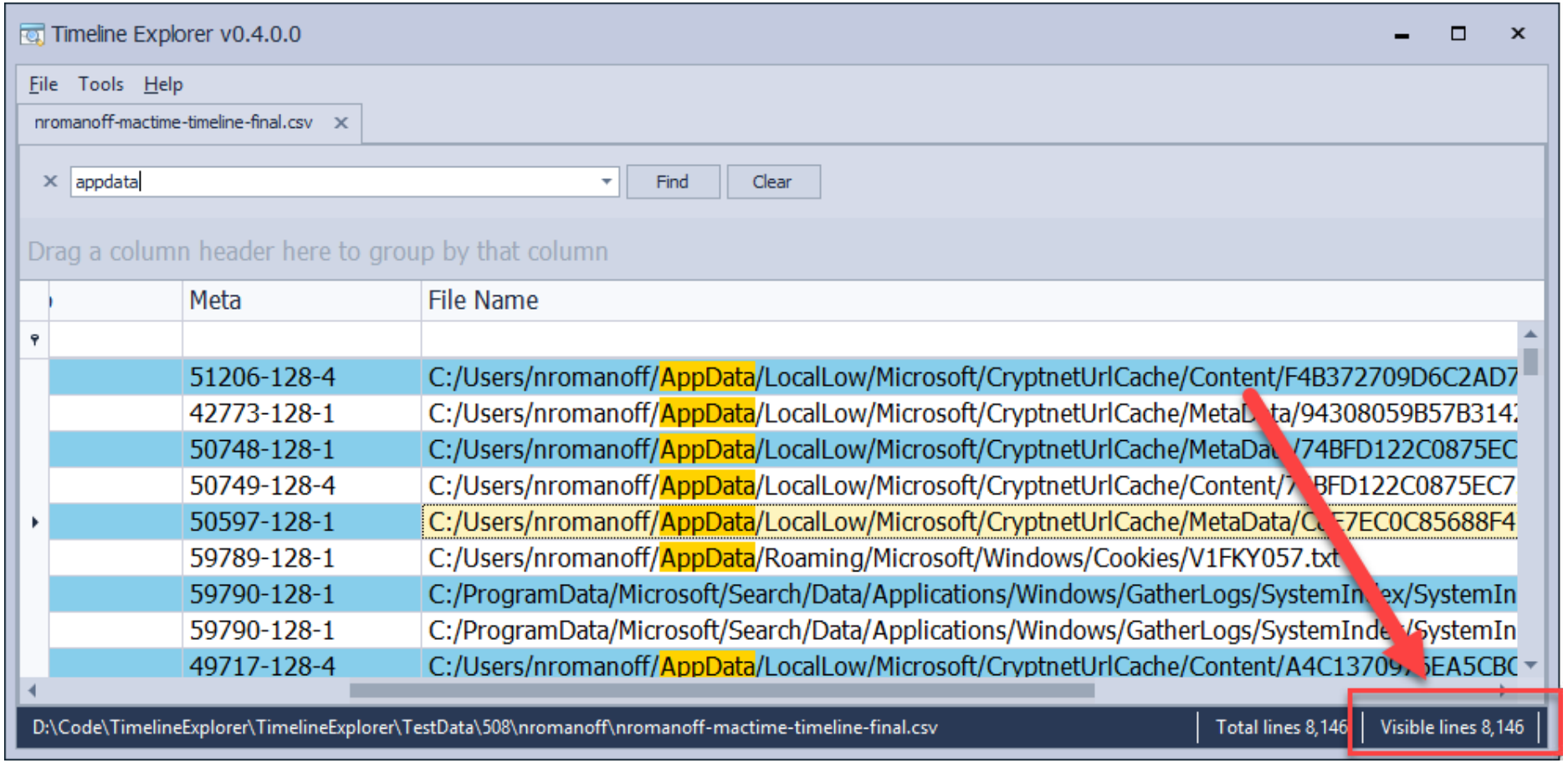
From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Timeline Explorer: Event Grouping Feature



From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Timeline Explorer: Event Searching Feature



From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Timeline Explorer: Event Searching Feature

Search help

When Match criteria is set to "Mixed" filtering works as follows. In its simplest form, a filter criterion consists of a single word. If you want to filter for a string containing a space character, specify this string in quotation marks. Without quotation marks, words separated by the space character are treated as individual conditions.

You can filter against a specific column by preceding a filter string with the column's display name plus a colon character.
ColumnDisplayName:FilterString

Instead of the complete name, it is possible to partially specify the display name, using the initial characters of a column's display name. A filter will be performed against the first column whose display name starts with the specified substring. If you want to filter against a column whose display caption contains space characters, specify the column's display caption in quotation marks.

If the filter string contains multiple conditions separated by space characters, and at least one condition defines a filter against a specific column, only records that match all of these conditions are shown (i.e., the conditions are combined by the AND logical operator). If there is no column specification, records that match at least one of these conditions are shown (i.e., the conditions are combined by the OR logical operator).

Precede a condition with "+" to display only records that match this condition. The "+" specifier allows you to implement the logical AND operator. There should be no space character between the "+" sign and the condition.

Precede a condition with "-" to exclude records that match this condition from the result set. There should be no space between the "-" sign and the condition.

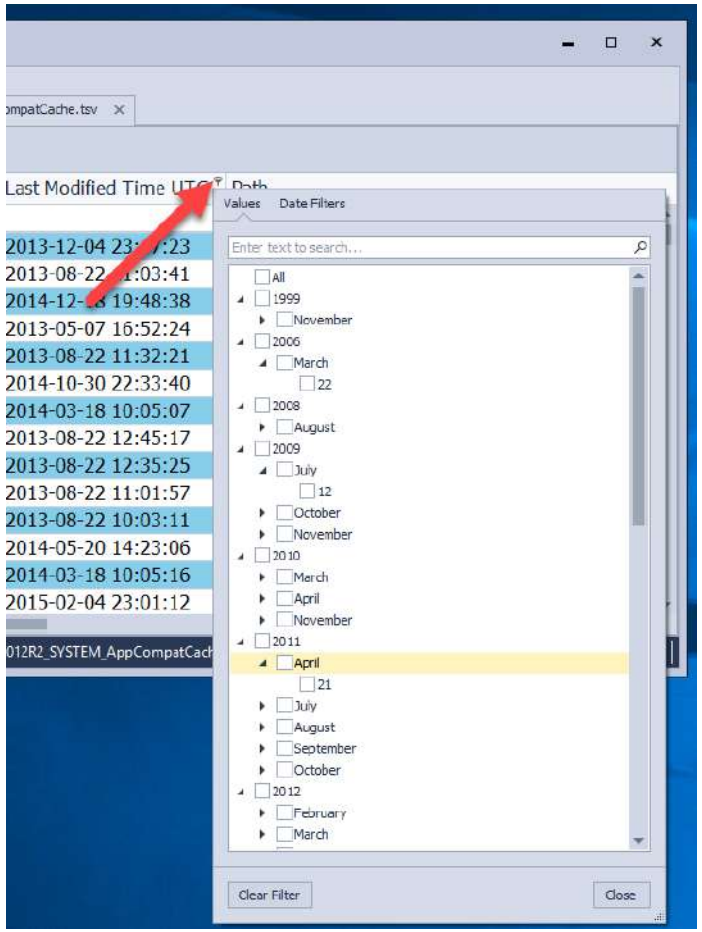
Changing the Match criteria to Or, And, or Exact negate the need to use - or + for these types of operations.

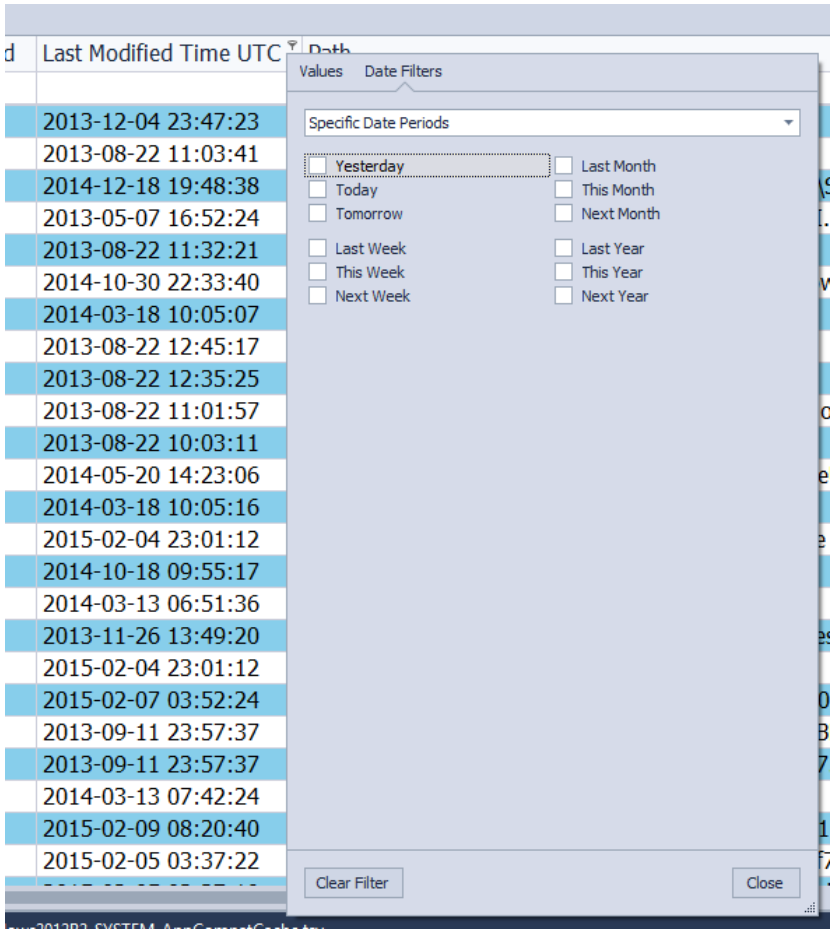
Examples

Search Criteria	Description
`register`	Selects records that contain the "register" string in any search column.
`check register Dave`	Selects records that contain either "check" OR "register" OR "Dave" strings in any search column.
`"check register"`	Selects records that contain "check register" in any search column.
`screen +"Richard Fisher"`	Selects records that contain both "screen" AND "Richard Fisher" in search columns.
`Product:Tofu Seattle`	Selects records that contain "Tofu" in the column that starts with "Product", AND also contain "Seattle" in any search column.
`data +entry -mark`	Selects records that contain both "data" AND "entry" in search columns, excluding records that contain "mark".
`menu mask -file`	Selects records that contain "menu" OR "mask", excluding records that contain "file".
`From:Roller Subj:"currency mask"`	Selects records that contain "Roller" in the column that starts with "From", AND also contain "currency mask" in the column that starts with "Subj".
`import -From:Steve`	Selects records that contain "import" in any search column, excluding records that contain "Steve" in the column that starts with "From".

From: https://aboutdfir.com/toolsandartifacts/windows/timeline-explorer/2/

Timeline Explorer: Event Filtering Feature





From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Timeline Explorer: Event Tagging Feature

File Tools Help

supertimeline.csv

Drag a column header here to group by that column

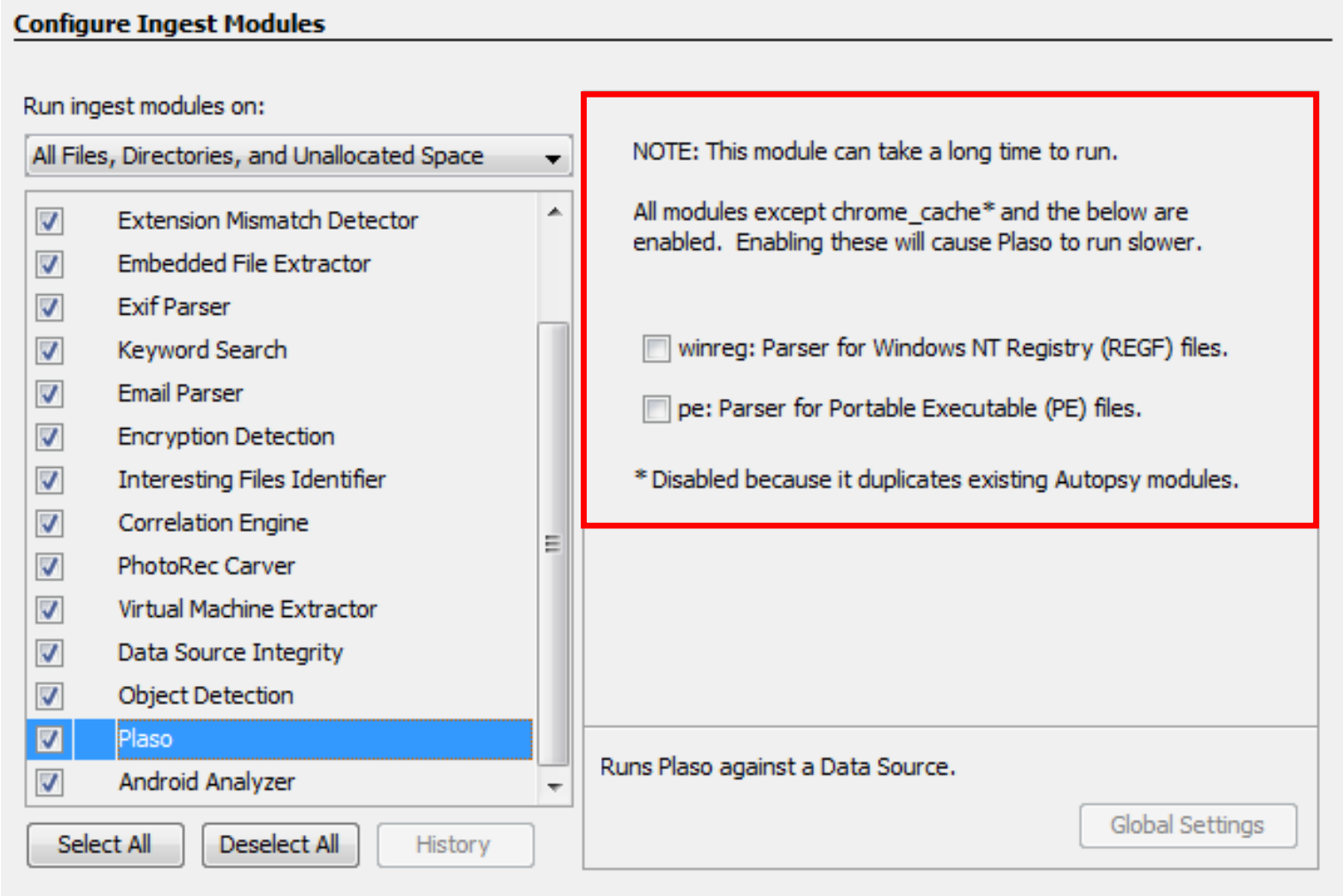
Line	Tag	Timestamp	Source Desc...	Source Name	macb	Inode	Long Description
2838	☐	2012-04-03 17:13:29	AppCompat...	REG	....	41356	[HKEY_LOCAL_MACHINE\System\Co
2839	☐	2012-04-03 17:13:29	WinEVTX	EVT	m...	41520	[7045 / 0x1b85] Record Number: 14
2840	☐	2012-04-03 17:13:29	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2841	☐	2012-04-03 17:13:29	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\IndexTable\File
2842	☐	2012-04-03 17:13:29	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2843	☐	2012-04-03 17:13:29	WinEVTX	EVT	m...	41520	[7036 / 0x1b7c] Record Number: 14
2844	☐	2012-04-03 17:13:29	WinEVTX	EVT	m...	41522	[4625 / 0x1211] Record Number: 52
2845	☐	2012-04-03 17:13:29	WinEVTX	EVT	m...	41522	[4776 / 0x12a8] Record Number: 52
2846	☐	2012-04-03 17:13:29	WinEVTX	EVT	m...	41520	[7036 / 0x1b7c] Record Number: 14
2847	☐	2012-04-03 17:13:40	WinEVTX	EVT	m...	41522	[4634 / 0x121a] Record Number: 52
2848	☐	2012-04-03 17:14:55	WinEVTX	EVT	m...	41522	[4672 / 0x1240] Record Number: 52
2849	☐	2012-04-03 17:14:55	WinEVTX	EVT	m...	41522	[4624 / 0x1210] Record Number: 52
2850	☑	2012-04-03 17:14:56	AppCompat...	REG	....	41356	[HKEY_LOCAL_MACHINE\System\Co
2851	☑	2012-04-03 17:14:56	AppCompat...	REG	....	41356	[HKEY_LOCAL_MACHINE\System\Co
2852	☐	2012-04-03 17:14:56	WinEVTX	EVT	m...	41520	[7045 / 0x1b85] Record Number: 14
2853	☐	2012-04-03 17:14:56	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\IndexTable\File
2854	☐	2012-04-03 17:14:56	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2855	☐	2012-04-03 17:14:56	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2856	☐	2012-04-03 17:14:56	WinEVTX	EVT	m...	41520	[7036 / 0x1b7c] Record Number: 14
2857	☑	2012-04-03 17:14:56	WinEVTX	EVT	m...	41522	[4776 / 0x12a8] Record Number: 52
2858	☐	2012-04-03 17:14:56	WinEVTX	EVT	m...	41522	[4625 / 0x1211] Record Number: 52
2859	☐	2012-04-03 17:14:56	WinEVTX	EVT	m...	41520	[7036 / 0x1b7c] Record Number: 14
2860	☐	2012-04-03 17:15:07	WinEVTX	EVT	m...	41522	[4634 / 0x121a] Record Number: 52
2861	☑	2012-04-03 17:16:07	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2862	☐	2012-04-03 17:16:07	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E
2863	☐	2012-04-03 17:16:07	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\LruList\000000
2864	☐	2012-04-03 17:16:07	UNKNOWN	REG	m...	41564	[\DefaultObjectStore\ObjectTable\6E

From: https://binaryforay.blogspot.com/2017/04/introducing-timeline-explorer-v0400.html

Autopsy's Plaso

- **Plaso ingest module**:
  - Runs Plaso to **generate events** that are displayed in the **Autopsy Timeline**
  - Various individual parsers: the slowest parsers by far are `winreg`, `pe`, and `chrome_cache`
  - In the module **configuration** panel: you can choose to enable the `winreg` and `pe` parsers
- Reference:
  - https://sleuthkit.org/autopsy/docs/user-docs/4.19.3/plaso_page.html

Plaso Module's Configuration



Source: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/plaso_page.html

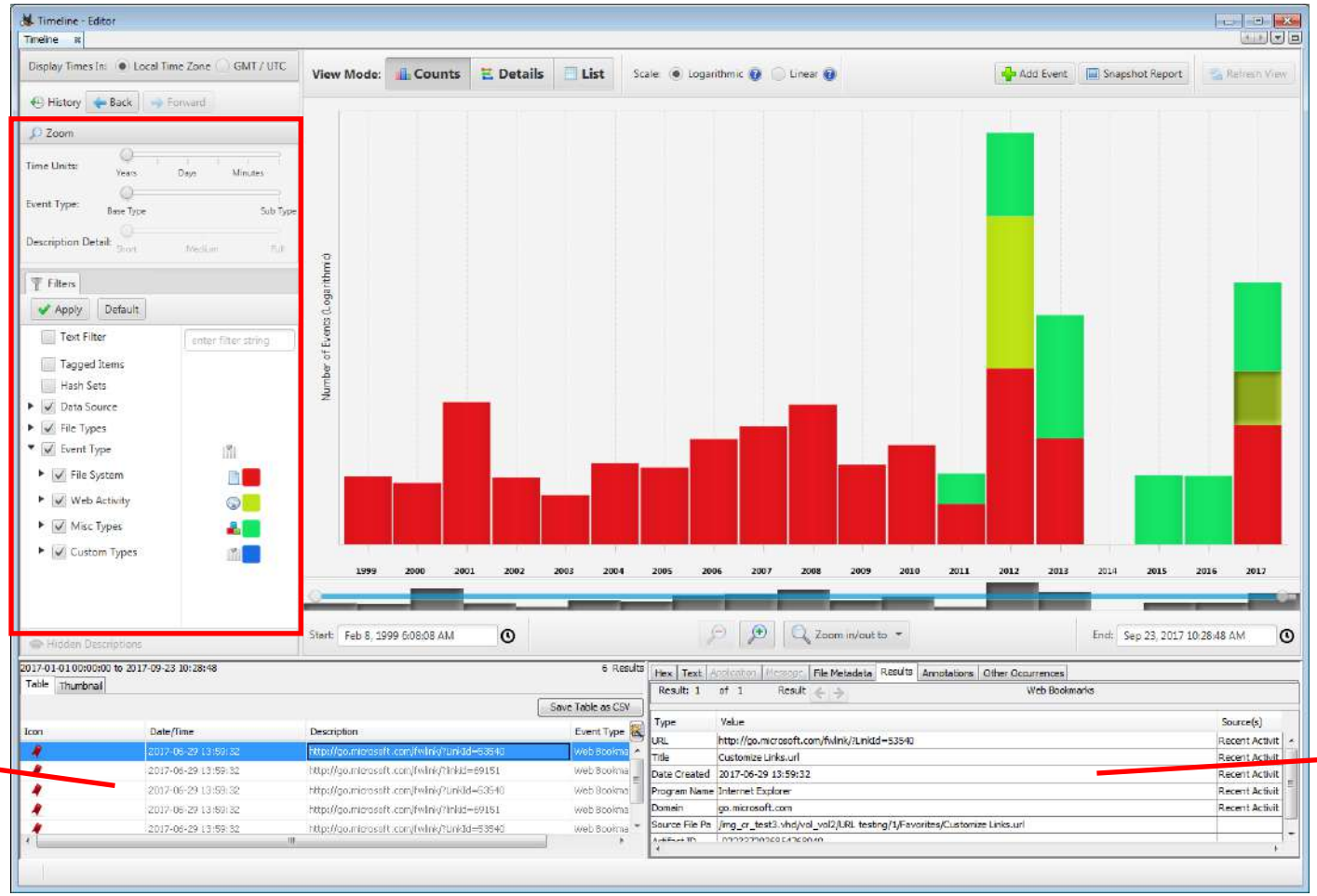
Autopsy's Timeline

- An "***event***": has a timestamp, a type, and a description
- The "***timeline***": collects data from **multiple sources** and **organizes** events into the following taxonomy:
  - **File system**: Modified, Access, Changed, Created
  - **Web activity**: web downloads, cookies, bookmarks (creation), history, searches, form auto fill, form address
  - **Miscellaneous**: messages, GPS routes, location history, calls, email, recent documents, installed programs, Exif metadata, devices attached, log entry, registry
- Reference:
  - http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html

Autopsy's Timeline: The *Counts View*

- A stacked bar chart showing **how much activity** occurred in a given time frame

Refer to Lab 8's Task 1 for the **UI controls**



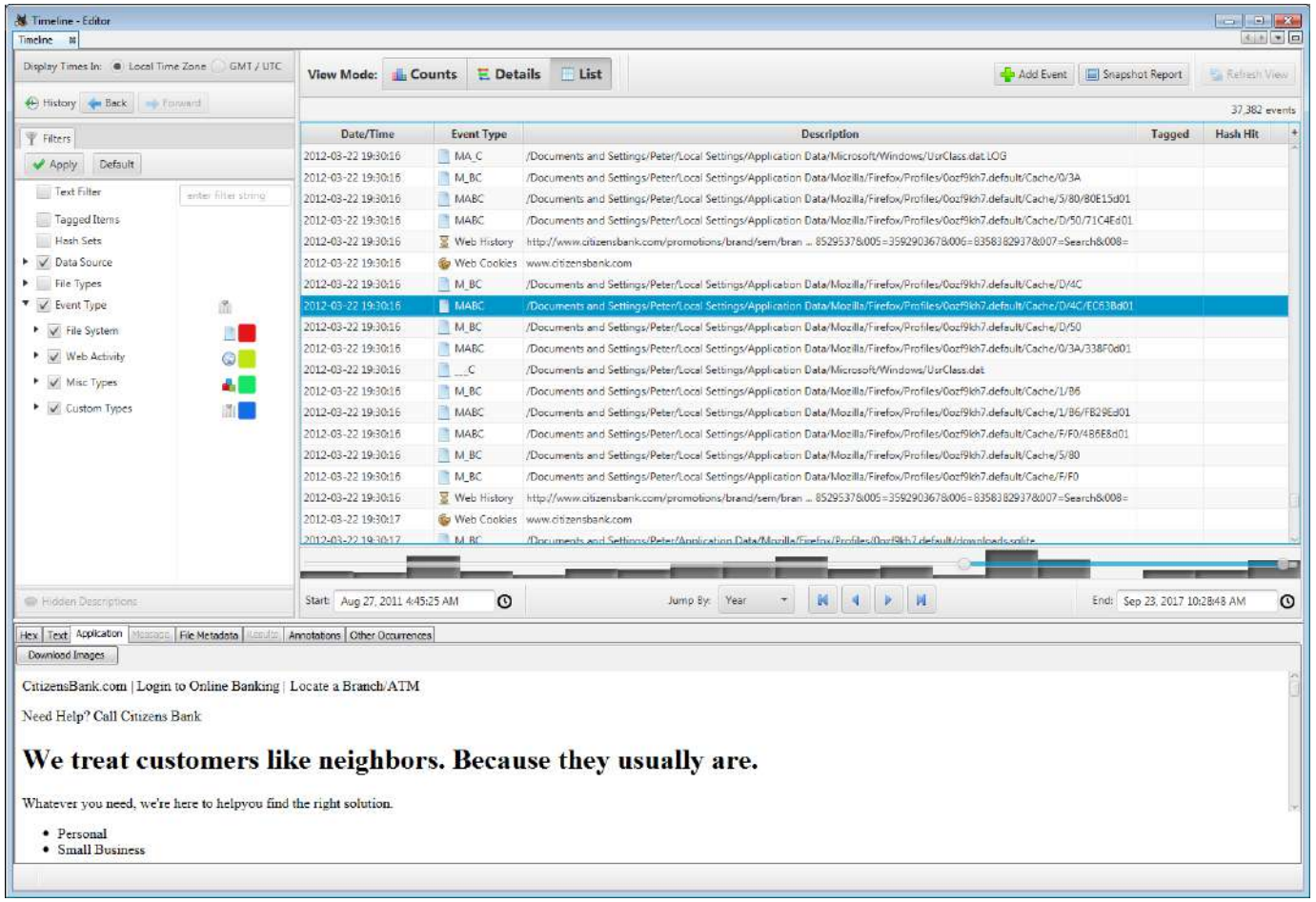
Source: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html

Result viewer (unavailable in the List view)

Content viewer

Autopsy's Timeline: The *List View*

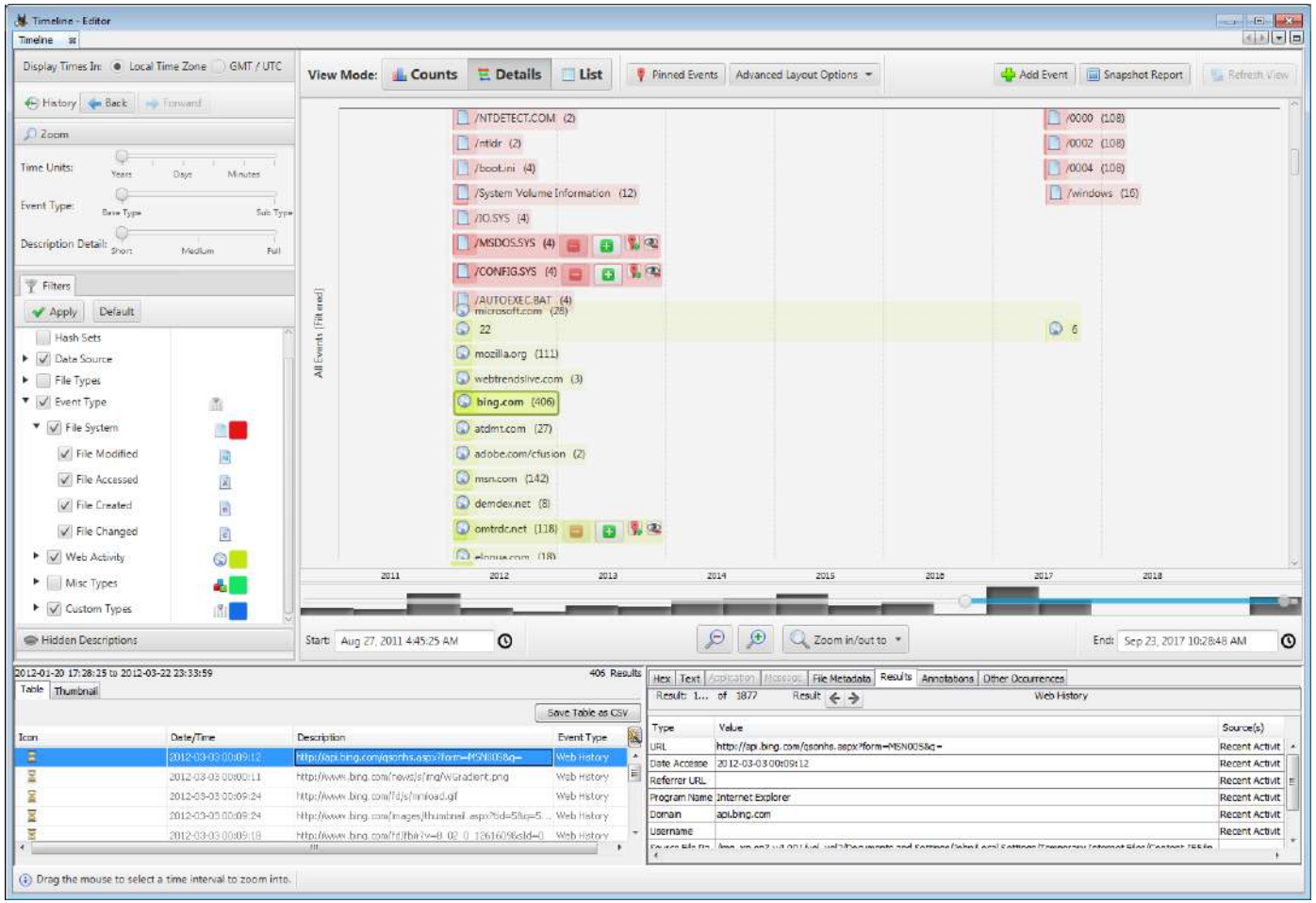
- It shows **all events** in the order they occurred



Source: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html

Autopsy's Timeline: The *Details View*

- It shows **individual or groups of related events** along the date/time x-axis

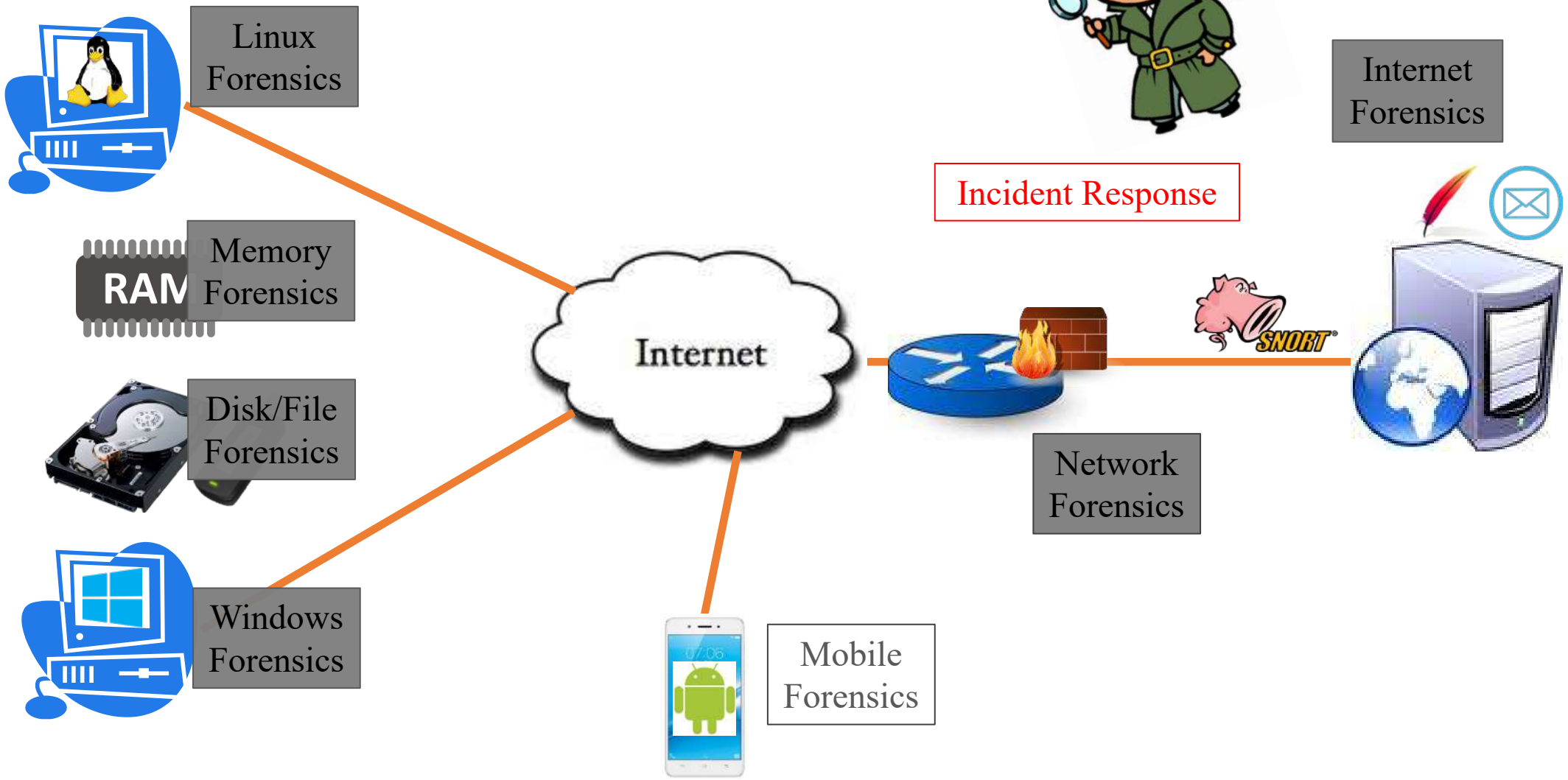


Source: http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/timeline_page.html

Break!

Incident Response

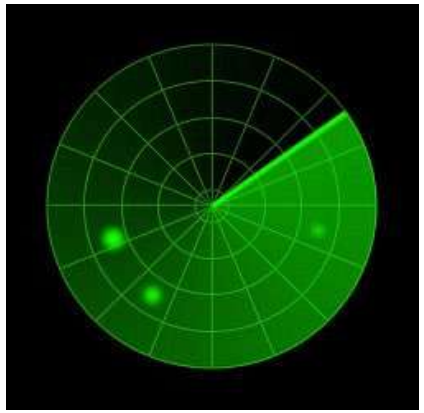
This Lecture's Focus



Big Picture of Attacks

Reconnaissance

Scanning



Break-in

Malware

Hiding

What is Incident Response?

- ***"Computer security incident"*** [NIST]:
  a violation or imminent threat of violation of:
  - Computer security policies;
  - Acceptable use policies; or
  - Standard security practices
- ***Incident Response/Management***:
  the **monitoring & detection** of ***security events***
  on a computer or computer network,
  and the execution of proper **responses** to those events

Incident Response Life Cycle

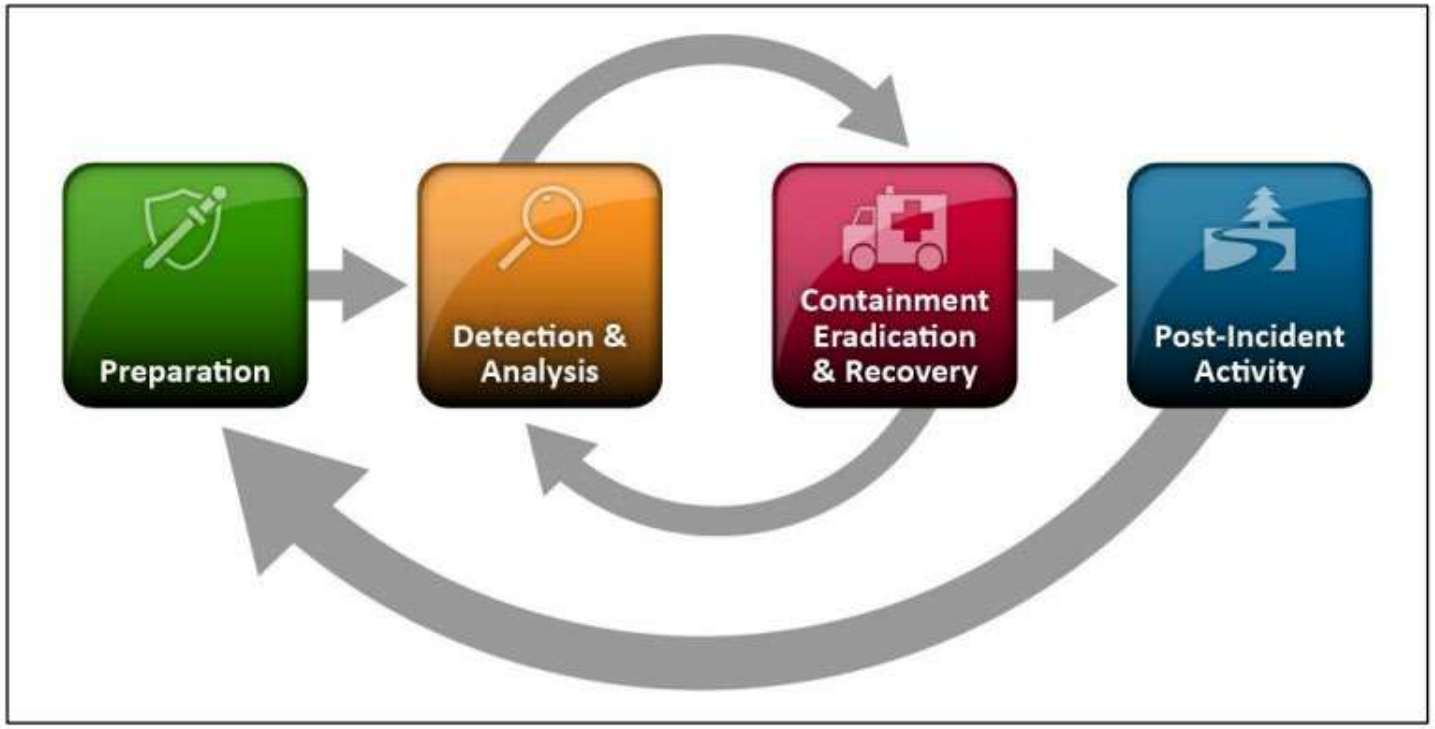


Figure 3-1. Incident Response Life Cycle

Reference: NIST, "*Computer Security Incident Handling Guide*", Special Publication 800-61, Revision 2

Incident Response Steps

- **Steps**:
  1. Preparation
  2. Detection & analysis
  3. Containment
  4. Eradication
  5. Recovery
  6. Post-incident activity

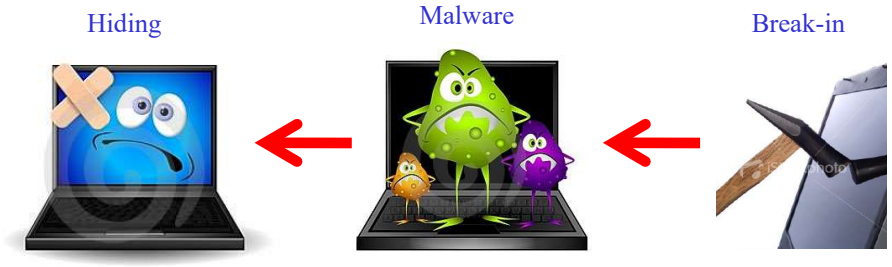
- More on IR steps:
  - "*The Basics of Incident Response*": https://www.youtube.com/watch?v=VTOoKBJX1Gs

Incident Response vs Digital Forensics

- **Digital forensics** (DF):
  - Data collection & analysis: **investigative**, **retrospective**, **preservative**
- **Incident Response** (IR):
  - Detection & analysis: **investigative**, **retrospective**
    (with less restrictions on performing live analysis – *less preservative*)
  - Containment, eradication: ***responsive***
  - Recovery: ***restorative***

- Various DF knowledge & skills are **relevant** to IR!
  - E.g., analysis of log events, registry keys, Windows artefacts, etc.
  - Our focus is on ***performing live analysis***
    for IR's detection & analysis steps

Common Attack Steps & System Objects



- **Initial access**:
  - Email, browser, RDP
- **Process execution**:
  - Prefetch, user assist, system caches, …
- **Payloads** (access on objectives):
  - Data theft (object access), file creation/modification, etc.
- **Persistence**:
  - Tasks, services, registry keys, user accounts
- **Lateral movement**:
  - RDP, remote access tools

Signs of Intrusion on a Windows Host

- Illegal **connections**
- Unusual **processes**
- Unusual **services**
- **Autostart** points
- Unusual **ports**
- Added/modified **user accounts**
- Unusual **files**
- Added/modified **registry entries**

What Windows Artefacts to be Inspected?

- To investigate ***past*** actions:
  - **Event log analysis**: remote access, account management, object access, scheduled tasks, process auditing, …
  - **Evidence of past program executions**: Windows registry, execution-related artefacts
- To check ***current/ongoing*** activities:
  - **Analysis** of system information, running processes, open files, network connections/activities, …
  - **Tools** to utilize: Windows commands, system-diagnostic tools from SysInternals, `wmic`

Event Log Analysis for Incident Response

- We’ve discussed Windows log analysis using **Event Viewer**
- Some **previously discussed** events:
  - **Logon** activities: 4624(S), 4625(F)
  - **Logoff** activities: 4634(S), 4647(S)
- Need to check events of ***commonly-done actions*** in an intrusion:
  - Remote access, including RDP
  - Program execution
  - Object access
  - Account management
  - Scheduled tasks

Event IDs and Categories

- There are ***so many*** event IDs in Windows!
- You can see the **list** of event IDs at:
- https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
- Or https://www.xplg.com/windows-server-security-events-list/
- Some ***event-ID categories***:
  account logon, account management, logon/logoff, object access, system, global object access auditing

- The next few slides give a ***partial list*** (just **for your reference**)
- To **check** a particular event ID ***XXXX***, please visit: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-*XXXX*
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

For Reference Only

Events Related to Remote Access & RDP

- **Kerberos authentication** events (part of **domain-account** logons):
  - **4768(S, F)**: A Kerberos **authentication ticket (TGT)** was requested
  - **4769(S, F)**: A Kerberos **service ticket was requested**
  - **4770(S)**: A Kerberos **service ticket was renewed**
  - **4771(F)**: Kerberos pre-authentication **failed**
  - **4772(F)**: A Kerberos **authentication ticket** request failed
  - **4773(F)**: A Kerberos **service ticket** request failed
  - **4776(S, F)**: The computer attempted to **validate the credentials** for an account
  - **4777(F)**: The domain controller failed to **validate the credentials** for an account
- References:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-kerberos-authentication-service
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-kerberos-service-ticket-operations
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-credential-validation

For Reference Only

Events Related to Remote Access & RDP

- **Logon** and **logoff** events:
  - **4624(S)**: An account was successfully **logged on**
  - **4625(F)**: An account **failed** to log on
  - **4634(S)**: An account was **logged off**
  - **4647(S)**: User initiated **logoff**
  - **4648(S)**: A **logon** was attempted using explicit credentials
  - **4672(S)**: Special **privileges** assigned to new logon
  - **4778(S)**: A session was **reconnected** to a Window Station
  - **4779(S)**: A session was **disconnected** from a Window Station
- References:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-logon
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-logoff
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-logonlogoff-events

For Reference Only

Events Related to Object Access

- **File-share** events:
  - **5140(S, F)**: A network **share object** was accessed
  - **5142(S)**: A network **share object** was added
  - **5143(S)**: A network **share object** was modified
  - **5144(S)**: A network **share object** was deleted
  - **5145(S, F)**: A network **share object** was checked to see whether client can be granted desired access
- References:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-share
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-detailed-file-share

For Reference Only

Events Related to Process Auditing

- **Process** and **network-access** events:
  - **4688(S)**: A **new process** has been created
  - **5031(F)**: The Windows Firewall Service blocked an **application** from accepting incoming connections on the network
  - **5152(F)**: The Windows Filtering Platform **blocked** a **packet**
  - **5154(S)**: The Windows Filtering Platform has **permitted** an application or service to **listen on a port** for incoming connections
  - **5156(S)**: The Windows Filtering Platform has **permitted** a **connection**
  - **5157(F)**: The Windows Filtering Platform has **blocked** a **connection**
  - **5158(S)**: The Windows Filtering Platform has **permitted** a **bind** to a local port
  - **5159(F)**: The Windows Filtering Platform has **blocked** a **bind** to a local port
- References:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-process-creation
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-filtering-platform-connection
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-filtering-platform-packet-drop

For Reference Only

Events Related to Computer-Account Management

- **Computer-account** management events:
  - **4741(S)**: A **computer account** was created
  - **4742(S)**: A **computer account** was changed
  - **4743(S)**: A **computer account** was deleted
- Reference:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-computer-account-management

For Reference Only

Events Related to User-Account Management

- **User-account** management events**:**
  - **4720(S)**: A **user account** was created
  - **4722(S)**: A **user account** was enabled
  - **4723(S, F)**: An attempt was made to change an **account's password**
  - **4724(S, F)**: An attempt was made to reset an **account's password**
  - **4725(S)**: A **user account** was disabled
  - **4726(S)**: A **user account** was deleted
  - **4738(S)**: A **user account** was changed
  - **4781(S)**: The **name** of an account was changed
- Reference:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-user-account-management

For Reference Only

Events Related to Security-Group Management

- **Security-group** management events**:**
  - **4731(S)**: A security-enabled **local group** was created
  - **4732(S)**: A member was added to a security-enabled **local group**
  - **4733(S)**: A member was removed from a security-enabled **local group**
  - **4734(S)**: A security-enabled **local group** was deleted
  - **4735(S)**: A security-enabled **local group** was changed
  - **4764(S)**: A **group's type** was changed
  - **4737(S)**: A security-enabled **global group** was changed
  - **4728(S)**: A member was added to a security-enabled **global group**

For Reference Only

Events Related to Security-Group Management

- **4754(S)**: A security-enabled **universal group** was created
- **4755(S)**: A security-enabled **universal group** was changed
- **4756(S)**: A member was added to a security-enabled **universal group**
- **4757(S)**: A member was removed from a security-enabled **universal group**
- **4758(S)**: A security-enabled **universal group** was deleted

- Reference:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management

For Reference Only

Events Related to Scheduled Tasks

- **Scheduled task** events**:**
  - **4698(S)**: A scheduled **task** was created
  - **4699(S)**: A scheduled **task** was deleted
  - **4700(S)**: A scheduled **task** was enabled
  - **4701(S)**: A scheduled **task** was disabled
  - **4702(S**): A scheduled **task** was updated
- Reference:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events

For Reference Only

Events Related to Registry-Object Access

- **Registry-object access** events:
  - **4656(S, F)**: A handle to an **object** was requested
  - **4657(S)**: A **registry value** was modified
  - **4658(S)**: The handle to an **object** was closed
  - **4660(S)**: An **object** was deleted
  - **4663(S)**: An attempt was made to **access** an object
- Reference:
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-registry

Event Log Analysis for IR: References

- **General** event log analysis:
  - Steve Anson, "*Applied Incident Response*", Wiley, 2020
  - SANS DFIR Webcast, "*Incident Response Event Log Analysis*": https://www.youtube.com/watch?v=Xw536W7kbDQ
- **Remote desktop** activity logs:
  - http://woshub.com/rdp-connection-logs-forensics-windows/
  - https://frsecure.com/blog/rdp-connection-event-logs/
- **Active Directory** monitoring:
  - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Past Program Executions in Windows

- We have discussed the following related to program executions:
  - Prefetch files
  - UserAssistregistry keys
- *Any other **relevant artefacts**?*
  - **AmCache**
  - Application Compatibility Cache (**AppCompatCache**) a.ka **ShimCache**
- Both are useful to Incident Response

AmCache

- A **registry file** storing the information of ***executed applications***, including: the execution path, first executed time, deleted time, and first installation
- **`Amcache.hve`:**
  - Replaces `RecentFileCache.bcf` (from Windows 8)
  - Uses the Windows NT **Registry File** (REGF) format
  - A common **location**: C:\Windows\AppCompat\Programs\Amcache.hve
- **AmcacheParser**: https://github.com/EricZimmerman/AmcacheParser
- Reference:
  - Eric Zimmerman, "(Am)Cache rules everything around me": https://www.youtube.com/watch?v=iTchBtRr6TA

AppCompatCache/ShimCache

- Used to identify application **compatibility issues** with **executables**, e.g. whether **shimming** is needed or not:
  - It stores various **file metadata** e.g.:
    the full file path, file size, last modified date & process execution flag
  - It only contains the information ***prior to*** the system's **last startup**:
    current entries are stored only in **memory**
- The **location** is in the following **registry key**:
  `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache`
- **AppCompatCacheParser**:
  https://github.com/EricZimmerman/AppCompatCacheParser
- Reference: https://www.mandiant.com/resources/caching-out-the-val, https://www.youtube.com/watch?v=ZKlyu-HOvxY

Windows Live Analysis: For Ongoing Attack

- Various useful tools for **live analysis**:
  - Windows commands
  - Windows GUI tools, e.g. Microsoft Management Console (MMC)
  - Various **SysInternals' tools**, including process monitoring tools
  - **Windows Management Instrumentation Command-line (WMIC)**

Windows Commands & SysInternals' Tools

- Display system date and time: `date`, `time`
- Display when was the system rebooted: `uptime`
- Display various system information: PsInfo
- Check network interface: `ipconfig`
- Check processes and services: `tasklist`, PsList, PsService, Process Explorer/Hacker
- List currently loaded DLLs: ListDLLs, Process Explorer/Hacker
- View open files: PsFile, `openfiles`
- Show network connections: `netstat`
- List logged in users: PsLoggedOn, LogonSessions
- …
- References:
  - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands
  - https://docs.microsoft.com/en-us/sysinternals/

Some GUI-based *Process-Monitoring* Tools

- There are various tools from **SysInternals**: https://docs.microsoft.com/en-us/sysinternals/
- For **process monitoring**:
  - Process Explorer
  - Autoruns
- Some other alternatives:
  - Process Hacker
- See: *Task 4 of Lab 8*

WMIC

- ***Windows Management Instrumentation (WMI)***:
  - "a set of **extensions** to the *Windows Driver Model* that provides an **OS interface** through which instrumented components provide **information & notification**"
  - Allows sys admin or incident handler to **retrieve data** about Windows system ***remotely***
  - Also allows for **operations** to be done on Windows system
- ***Windows Management Instrumentation Command-line (WMIC)*** interface/utility:
  - It was introduced in Win XP Professional
  - The namespace is very **rich**, but can be **too complex**
  - For our purposes, we need to understand the **command syntax & usage**
  - We can focus on a **subset** of full WMI capabilities

WMIC: Command Syntax

- WMIC **commands**:
  - Are case **insensitive**
  - Can run in ***non-interactive*** mode:
    a **single command** issued at a cmd.exe or PowerShell console prompt
  - Can apply to **local** machine or **remote** machine(s) via global switches
- **General syntax**:
  `wmic` [*global-switches*] <*WMI-class-alias*> [*WQL-filter*]
  <*verb*> <*verb-arguments*>
- If you need **help**:
  - `wmic /?`
  - https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmic

WMIC Command: Global Switches

- Some important **switches**:
  - **/NODE**: Computer names, comma delimited
  - **/FAILFAST on**: Computers are pinged before sending WMIC commands
  - **/USER:<*username*>**: User name used when accessing the /NODE computers; you are prompted for the password
  - **/PASSWORD:<*password*>**: Password used when accessing the /NODE computers; the password is **visible** at the command line (please ***don't use*** this switch!)
  - **/OUTPUT:<*filename*>|STDOUT|CLIPBOARD**: For all output redirection
  - **/APPEND:<*filename*>|STDOUT|CLIPBOARD**: For all output redirection but *append* rather than *overwrite* if data already exists

WMIC Command: WMI-Class Aliases

- Some commonly used **aliases**:
  - **BIOS**: The BIOS system
  - **COMPUTERSYSTEM**: The target computer system
  - **ENVIRONMENT**: System environment variables
  - **GROUP**: Groups
  - **LOGICALDISK**: Volumes and file systems
  - **NICCONFIG**: Network card and networking configuration
  - **OS**: Installed OS
  - **PROCESS**: Running processes
  - **PRODUCT**: Software products installed
  - **SERVICE**: Services
  - **USERACCOUNT**: User accounts

WMIC Command: WMI Query Language (WQL)

- ***WMI Query Language (WQL)***:
  - A subset of ANSI SQL
  - **WHERE clause** for WQL filtering: e.g. `where "name='svchost.exe'"`
  - The use of the single and double quotes can be reversed
  - WQL **operators**: =, <, >, IS, IS NOT, LIKE
- Reference:
  - https://docs.microsoft.com/en-us/windows/win32/wmisdk/wql-sql-for-wmi

WMIC Command: Verbs

- Some commonly used **verbs**:
  - **ASSOC**: Return instances associated with the object
  - **CALL**: Executes a method
  - **CREATE**: Creates a new instance, and sets the property values
  - **DELETE**: Deletes the current instance or set of instances
  - ***GET***: Retrieves specific property values
  - **SET**: Assigns values to properties
  - ***LIST***: Shows data, this is the **default** verb
- For the verb **arguments**:
  - `wmic` <*WMI-class-alias*> <*verb*> `/?`

WMIC Usage

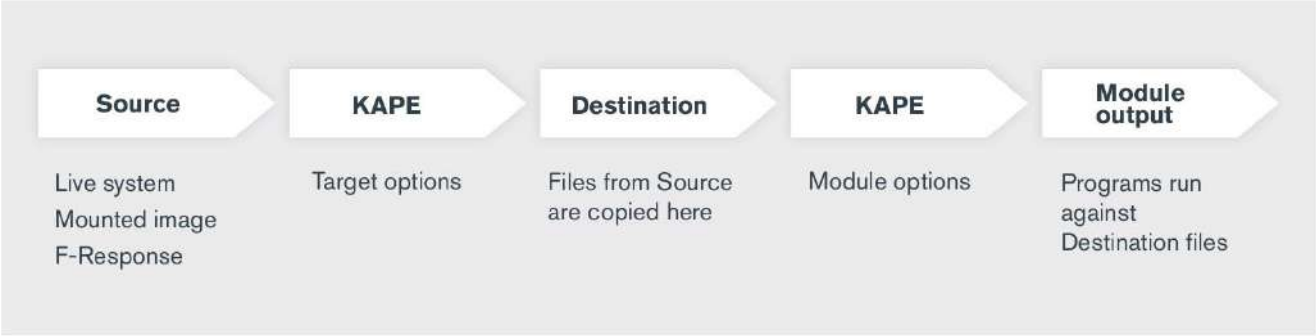
- Some commands for **basic usage**:
  - See Lab 8 Task 3
- Useful **video** for complex analysis:
  - "*The ABCs of WMI - Finding Evil in Plain Sight*", https://www.youtube.com/watch?v=k-_O59BnsHg

The Problem: *So Many Tools!*

- You can check, for example, **EZ Tools**: https://ericzimmerman.github.io/#!index.md
- Various developed **parsers/extractors/explorers**:
  - AmcacheParser: Amcache.hve parser
  - ApCompatCacheParser: AppCompatCache/ShimCache parser
  - PECmd: Prefetch parser
  - MFTECmd: MFT extractor/parser
  - SBECmd: ShellBags explorer
  - … (*ECmd) ☺
- *Question: How to perform various IR tasks fast?*
- An ***IR triage* suite**

Kroll Artifact Parser and Extractor (KAPE)

- Created by Kroll director, Eric Zimmerman
- An accompanying GUI tool named **Gkape**
- It lets IR teams **collect/extract** & **process/parse** artifacts from a device or storage location *within minutes*:



Source: https://ericzimmerman.github.io/KapeDocs/#!index.md

- KAPE's project and documentation sites:
  - Project site: https://github.com/EricZimmerman/KapeFiles
  - Documentation site: https://ericzimmerman.github.io/KapeDocs/#!Pages%5C2.-Getting-started.md

How Popular is KAPE?

- From: https://forensic4cast.com/forensic-4cast-awards/

The awards ceremony was held at the SANS DFIR Summit in Austin on July 26, 2019.

The winners of the awards are marked in **BOLD** below:

DFIR Commercial Tool of the Year

- ***Magnet Forensics***
- Cellebrite
- X-Ways Forensic

DFIR Non-commercial Tool of the Year

- Volatility
- Autopsy
- ***Eric Zimmerman Tools***

The awards ceremony was held at the SANS DFIR Summit on July 17, 2020.

The winners of the awards are marked in **BOLD** below:

DFIR Commercial Tool of the Year

- **Magnet AXIOM**
- Cellebrite UFED Ultimate
- Belkasoft Evidence Center

DFIR Non-commercial Tool of the Year

- Kape
- **Autopsy**
- iLEAPP

The 2021 Forensic 4:cast Awards took place on Friday, July 23, 2021 as part of the SANS DFIR Summit. The nominees and **winners** are listed below:

DFIR Commercial Tool of the Year

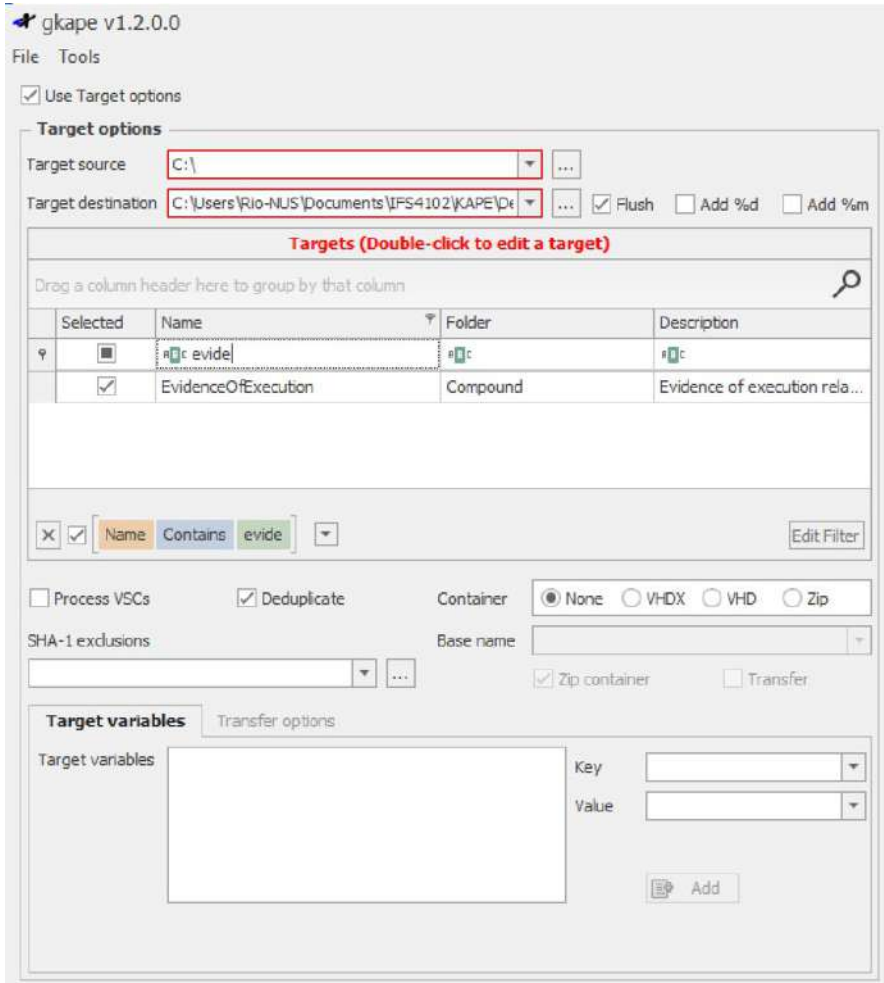
- **Magnet Forensics**
- Cellebrite
- Belkasoft

DFIR Non-Commercial Tool of the Year

- Kape
- **Autopsy**
- WinTriage

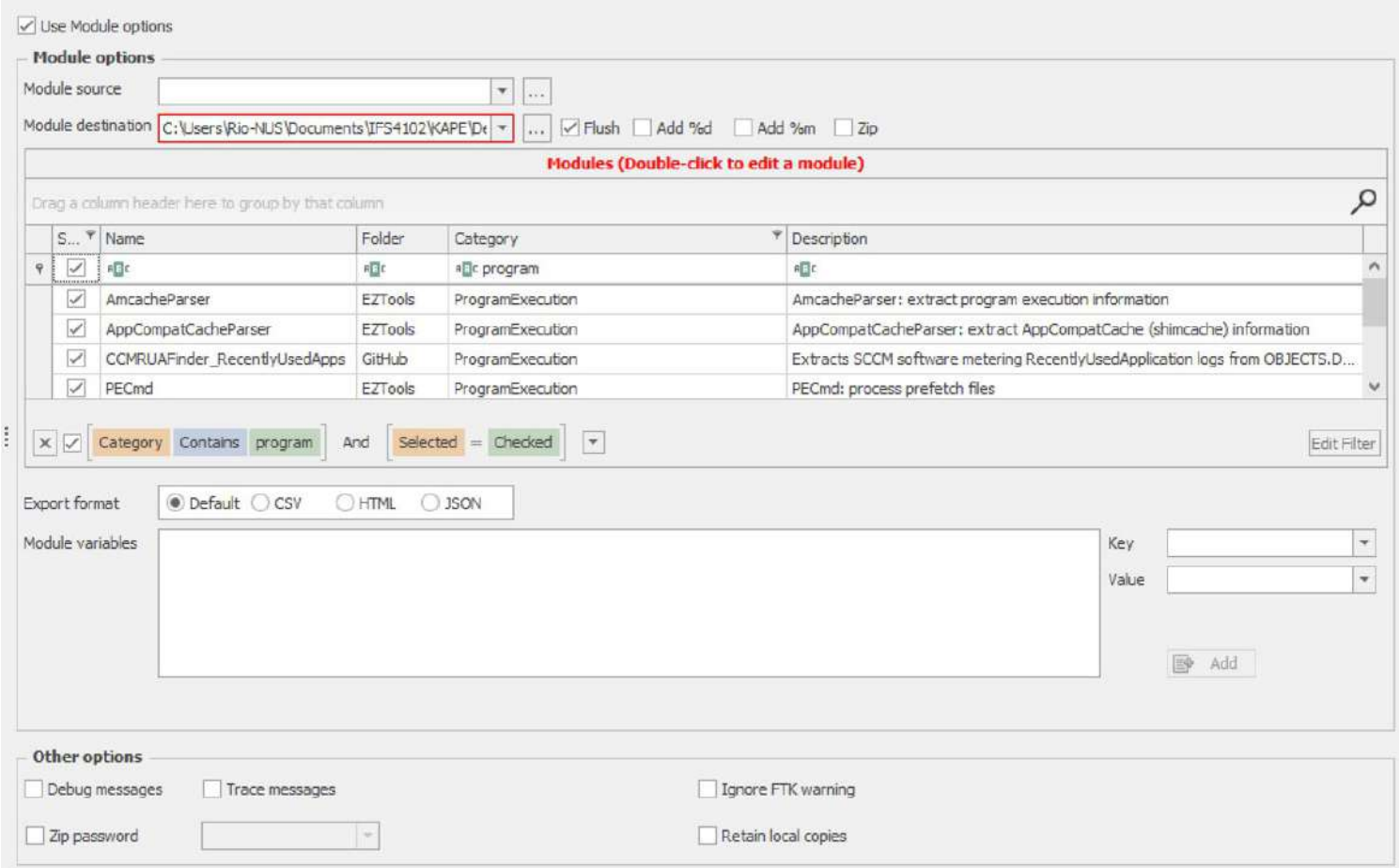
Using KAPE

- **Targets**: tell KAPE where to grab certain forensically important files



Using KAPE

- **Modules**: parsers for the files copied to the Target Destination folder



KAPE: Additional References

- References on **KAPE usage**:
  - John Davis, "*How to use KAPE for Fast and Flexible Incident Response*", https://www.giac.org/paper/gcih/34611/kape-fast-flexible-incident-response/152146
  - KAPE: https://aboutdfir.com/toolsandartifacts/windows/kape/

- **Video**:
  - "*Introduction to KAPE*": https://www.youtube.com/watch?v=pZRrZAJif8Q

Lab 8 Exercises

- Task 1: Using Autopsy's **Plaso** ingest module & **Timeline** feature
- Task 2 (*optional*): Conducting a **timeline analysis** on time-containing artefacts & disk image file using **Log2timeline/Plaso** + **Timeline Explorer**
- Task 3: Running various Window's **wmic** commands
- Task 4 (*optional*): Using process-monitoring tools in Windows, including **Process Explorer**, **Process Hacker** & **Autoruns**
- Task 5: Using **KAPE** for evidence extraction & parsing

Questions?
See you next week!