

CYB402 DIGITAL EVIDENCE FORENSIC WEEKLY REPORT

John Smith

513 Wallaby Way

Section 1: FICTITIOUS CASE INFORMATION

Case #: 234 CIS Number 38365

Cloud Breach	No	Server Breach	Yes	Remedy:	Yes
--------------	----	---------------	-----	---------	-----

Distribution: ☒ Server ☐ laptop ☐ External-Audit ☒ IT ☒ Hard-drive ☐ Internal Audit
☐ Emp. Data Audit ☐ PC ☐ Other:

Date/Time Report Completed: 4/4/2022 8:00 AM Date/Time Incident Occurred: 1/3/2022 4:45 AM

Type of Report:

PARTIES INVOLVED:

<input checked="" type="checkbox"/> Involved	<input type="checkbox"/> Witness	<input type="checkbox"/> Complainant	<input type="checkbox"/> Mentioned
Name:	Last: Cobb	First: Bob	Title: Data Analyst
Company:	Wired Inc.	Email: bobsmith@gmail.com	
Cell Phone:	235-135-6313	Work Phone: 362-324-6323	Address: 513 Pie Ln.

<input type="checkbox"/> Involved	<input checked="" type="checkbox"/> Witness	<input type="checkbox"/> Complainant	<input type="checkbox"/> Mentioned
Name:	Last: Cobb	First: Hunter	Title: Data Analyst
Company:	Wired Inc.	Email: huntercobb@gmail.com	
Cell Phone:	724-426-2135	Work Phone: 631-631-3852	Address: 531 Stephanie St.

<input type="checkbox"/> Involved	<input type="checkbox"/> Witness	<input type="checkbox"/> Complainant	<input checked="" type="checkbox"/> Mentioned
Name:	Last: Hunt	First: Riker	Title: Sr. Data Analyst
Company:	Wired Inc.	Email: Riker@gmail.com	
Cell Phone:	642-246-4865	Work Phone: 246-538-2346	Address: 2356 Hills Rd.

[Agency] Case #:

SUMMARY: The evidence found included a phishing email which led to a download of a key logger onto our local company servers. Through wireshark we were able to identify where this threat came from.

EVIDENCE SUBMITTED:

Item # 1	Phishing Email
Item # 2	Malware on Server
Item # 3	Network connection via wireshark
Item # 4	
Item # 5	
Item # 6	
Item # 7	
Item # 8	

[insert scanned signature here]
Insert Name
Insert Title

[Agency] Case #:

Section 2: SOFTWARE UTILIZED

All software utilized in this examination is fully licensed and registered to [Fictitious Agency Name] or its agents. All software and forensic hardware has been validated pursuant to [Fictitious Agency Name] policies and procedures.

FORENSIC EXAMINATION OF EVIDENCE ITEM #1

SANS SIFT – Disk Imaging Tool

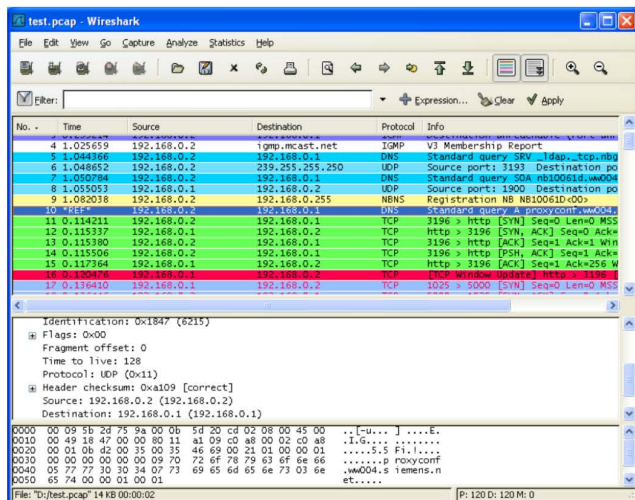
```
remnux@remnux:~$ sudo sifft install --mode=packages-only
> sifft-cli61.10.0+0-g48a701b
> sifft-version: not installed

> mode: packages-only
NOTICE: Fixing incorrect Saltstack version configuration.
Installing and configuring Saltstack properly ...
> downloading v2021.4.4
>> downloading sifft-saltstack-v2021.4.4.tar.gz.asc
>> downloading sifft-saltstack-v2021.4.4.tar.gz.sha256
>> downloading sifft-saltstack-v2021.4.4.tar.gz.sha256.asc
>> downloading sifft-saltstack-v2021.4.4.tar.gz
> validating file sifft-saltstack-v2021.4.4.tar.gz
> validating signature for sifft-saltstack-v2021.4.4.tar.gz.sha256
> extracting update sifft-saltstack-v2021.4.4.tar.gz
> performing update v2021.4.4
>> Log file: /var/cache/sifft/cli/v2021.4.4/saltstack.log

>> Running: software-properties-common
>> Running: apt-transport-https
>> Running: deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable
>> Running: sifft-gift-dev
>> Running: sifft
>> Running: /etc/apt/preferences.d/gift
>> Running: sifft-stable
```

FORENSIC EXAMINATION OF EVIDENCE ITEM #2

Wireshark – Used to monitor network connections

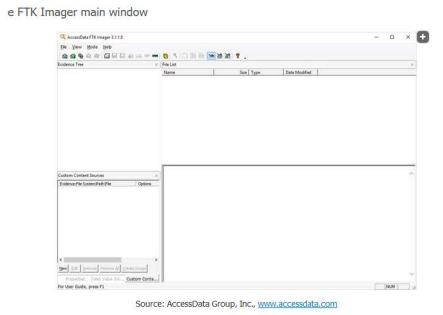


[insert scanned signature here]
Insert Name
Insert Title

[Agency] Case #:

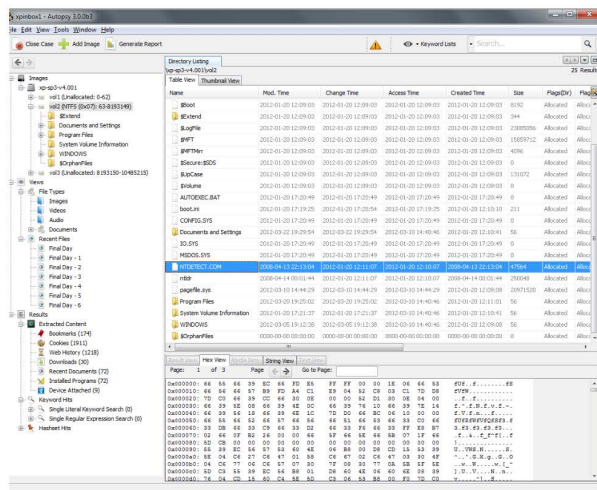
FORENSIC EXAMINATION OF EVIDENCE
ITEM #3

FTK Imager – Used to image disk media so that they can be duplicated and worked on.



FORENSIC EXAMINATION OF EVIDENCE
ITEM #4

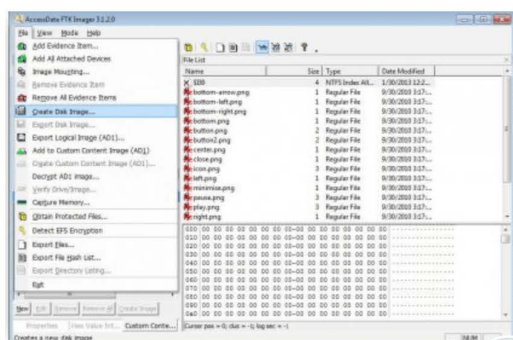
Autopsy – Digital forensic tool used to recover data.



FORENSIC EXAMINATION OF EVIDENCE
ITEM #5

FTK Imager – Another disk imaging tool

[Agency] Case #:



FORENSIC EXAMINATION OF EVIDENCE ITEM #6

Item #6 – Can be described as

[insert photo here]
[insert photo here]

[insert photo here]
[insert photo here]

FORENSIC EXAMINATION OF EVIDENCE ITEM #7

Item #7 – Can be described as

[insert photo here]
[insert photo here]

[insert photo here]
[insert photo here]

FORENSIC EXAMINATION OF EVIDENCE ITEM #8

Item #8 – Can be described as

[insert photo here]
[insert photo here]

[insert photo here]
[insert photo here]

[insert scanned signature here]
Insert Name
Insert Title

[Agency] Case #:

Section 3: DATA BREACH

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

NETWORK SERVER BREACH

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

- ☐ No Network Server breach detected.
- ☒ Network Server breach detected. If checked, identify and report on malware located below.

NETWORK BREACH

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

- ☐ No Network breach detected.
- ☒ Network breach detected. If checked, identify and report on malware located below.

CLOUD BREACH

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

- ☒ No Cloud breach detected.
- ☐ Cloud breach detected. If checked, identify and report on malware located below.

DATABASE BREACH

The original media was scanned for malware. Prior to the scan, all malware definitions were updated. The results were:

- ☐ No Database breach detected.
- ☒ Database breach detected. If checked, identify and report on malware located below.

BIOS EXAMINATION

Once the hard drive was removed, the computer was turned on and the BIOS (Basic Input/Output System) checked. The following was found:

- ☒ The date and time were accurate.
- ☐ The date was accurate, but the time was inaccurate. List time offset from correct time: _____
- ☐ The time was accurate, but the date was inaccurate. List date offset from correct date: _____
- ☐ From basic computer was adjusted to compensate for any time difference.

Insert scanned signature here

Insert Title

OFFICIAL USE ONLY

[Agency] Case #:

- ☒ Cellular phone set by network.
☒ Other used as a time reference:

VIRUS AND MALWARE

The original media was scanned for malware. Prior to the scan, all malware definitions were updated.
The results were:

- ☐ No malware detected.
☒ Malware detected. If checked, identify and report on malware located below.
A keylogger and trojan were detected.

VIRUS AND MALWARE TOOLS USED TO SCAN MEDIA

The original media was scanned for malware. Prior to the scan, all malware definitions were updated.
The results were:

- ☒ Wire Shark
☒ Vulnerability Scanner
☐ AppSec Stach
☐ NetSparker
☐ Nessus
☐ Other
☐ Malware detected. If checked, identify and report on malware located below.

[insert scanned signature here]
Insert Name
Insert Title

[Agency] Case #:

FORENSIC IMAGING**Section 4: FORENSIC EXAMINATION OF FILES**

After obtaining the hash value(s) of the original media, a forensic image was created. The forensic image was placed on a:

- ☐ Government owned, forensically wiped hard drive
- ☐ Government owned, forensically wiped Storage Area Network (SAN)
- ☐ Fictitiously owned company, wiped hard drive
- ☒ Fictitiously owned private, wiped hard drive

The forensic imaging software utilized in this process creates an imaging report, detailing the hash value(s) of the newly created forensic image. The hash value(s) of the forensic image was compared to the original hash value obtained prior to imaging the device. The hash value(s) of the forensic image:

- ☐ Matched exactly the hash value(s) of the original media.
- ☒ Did not match the original hash value(s) of the media. If checked, provide explanation below.

HASH OF ORIGINAL EVIDENCE

The original media was connected to a forensic hardware write blocker (fictitious asset tag #) and the write blocker connected to a forensic computer (asset tag #). Prior to doing anything with the original media, the media was hashed to obtain a baseline hash value. This allows the hash value of the original media to later be compared to the hash value of the forensic image created of the original media. By comparing the hash values of the original media and that of the forensic image, the forensic image can be authenticated as an exact duplicate copy of the original evidence.

The hash values obtained from the original evidence were as follows: (Sample only. Write your own!)

- ☒ MD5: asdf6fdsha534
- ☐ SHA1:
- ☐ Other:

DISPOSITION**EVIDENCE DISPOSITION**

The evidence collected includes records of network intrusions and downloaded files onto our computers that are malicious.

FORENSIC EXAMINER'S CONCLUSION/SUMMARY:

In conclusion, we have found a keylogger that found its way onto our network via a phishing link. Through the link it downloaded itself, uploaded it to our network, and replicated itself so that it could spread to every connected device on the network.

[insert scanned signature here]

DISPOSITION

Insert Title

[Agency] Case #:

ATTACHMENTS

APPROVALS

Report Author Digital Signature: Tyler C
Signature: Tyler C

Report Approver Digital

[insert scanned signature here]
Insert Name
Insert Title