BTSF

Evidence – Diego RIVERO

Contract number 2017 96 05 – New Food Investigation Techniques – Phase II - *Course 2a: E-Commerce of food standard*

European Commission

BTSF Evidence

- Collection
- Preservation
  - The hash code
- Presenting in document form
- Archiving

BTSF Collecting evidence

- Evidence collection must be traceable and well documented. Most when is based on volatile data.
- We have to avoid compromise the evidence. Either during collection or preservation.
- Before collecting evidence prepare the scenario (time, place, parties, tools, forms, etc.). Maybe you won't have more opportunities…

BTSF Collecting evidence

Ideally every digital evidence item should comply with:

- Continuity and validation
  - Proper recording of the chain of custody
  - Rigorous and complete records.
- Repeatability and reproducibility:
  - Repeatability: get the same results on the same testing environment.
  - Reproducibility: get the same test results on a different testing environment

BTSF Collecting evidence

- ✓ Chain of custody and integrity of digital evidence play an important role on investigation.
- ✓ Sensitive variable: “time”
- ✓ Digital evidence integrity
  - ✓ Integrity: property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source”

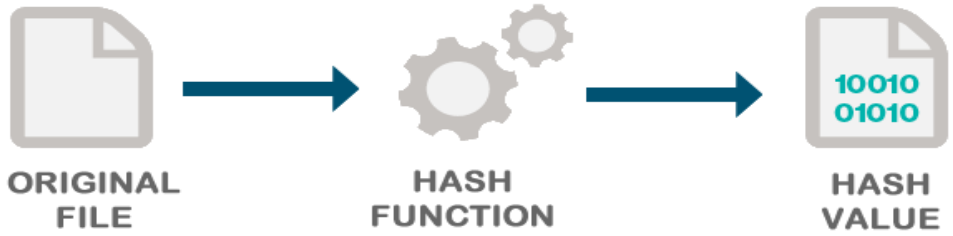
BTSF Collecting evidence

- Digital evidence in court… What is your experience? How do you prove the time/date of the digital evidence?
  - ✓ Reliability of the organization?
  - ✓ Log/report activity?
  - ✓ Cross-evidence?
  - ✓ Dual tool verification?
- How do you proof the integrity of the evidence? Have you ever had any problem?
  - ✓ Hash function?
  - ✓ Digital signing?

BTSF Evidence preservation

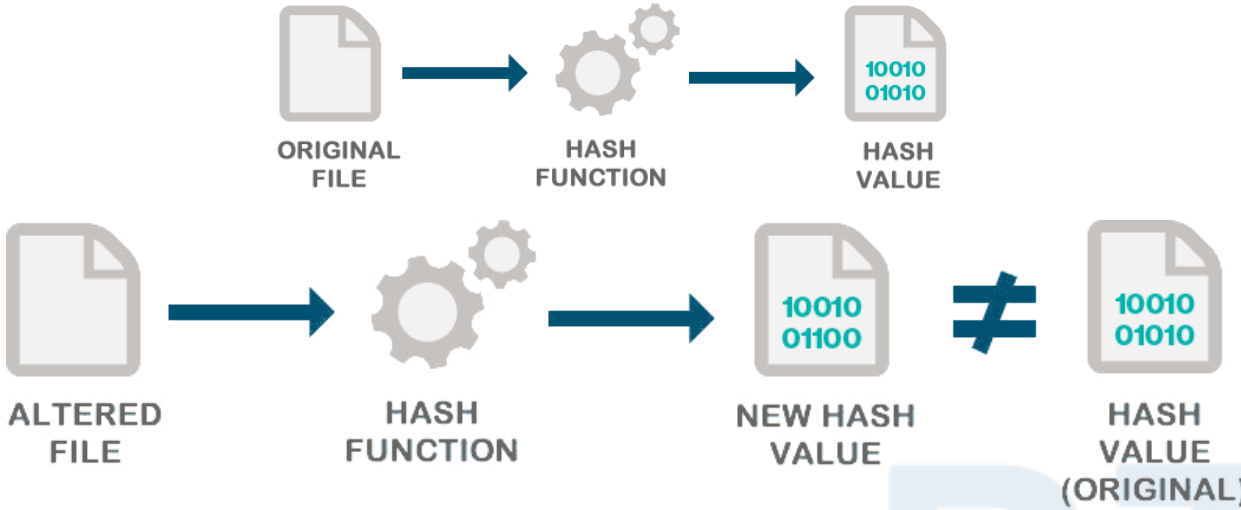
- Even more important than collection.
- Do backups and never, ever work with original copies.
- Use external parties if possible (public Notaries or third confidence parties).
- Calculate hash code of every piece of evidence.

BTSF Evidence preservation: Hash code



- Mathematical algorithm that calculates the value (a unique string of characters) if a file or group of files, based on its/their content.
- The string is called the '**hash** value', 'message digest', 'digital fingerprint', 'digest' or 'checksum'
- Provide trust in evidence.

BTSF Evidence preservation: Hash code



- Easy to identify if evidence has changed. If file content changes even a bit (0 or 1), the hash value changes.

BTSF Evidence preservation: Hash code

- Many cryptographic hash functions which returns alphanumeric string of different sizes. Most populars:

Hash function	Length	Example
MD5	128 bits	8B1A9953C4611296A827ABF8C47804D7
SHA-1	160 bits	F7FF9E8B7BB2E09B70935A5D785E0CC5D9D0ABF0
SHA-256	256 bits	185F8DB32271FE25F561A6FC938B2E264306EC304EDA518007D1764826381969
SHA-384	384 bits	3519FE5AD2C596EFE3E276A6F351B8FC0B03DB861782490D45F7598EBD0AB5FD5520ED102F38C4A5EC834E98668035FC
SHA-512	512 bits	3615F80C9D293ED7402687F94B22D58E529B8CC7916F8FAC7FDDF7FBD5AF4CF777D3D795A7A00A16BF7E7F3FB9561EE9BAAE480DA9FE7A18769E71886B03F315

BTSF Exercise: Calculating the hash code

Operating system (Windows)

Command Prompt

- Command tool:

  certUtil -hashfile pathToFileToCheck [HashAlgorithm]

- HashAlgorithm choices:

  MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

NOTE: Use quotation marks around file paths where spaces are used in file names or folder names

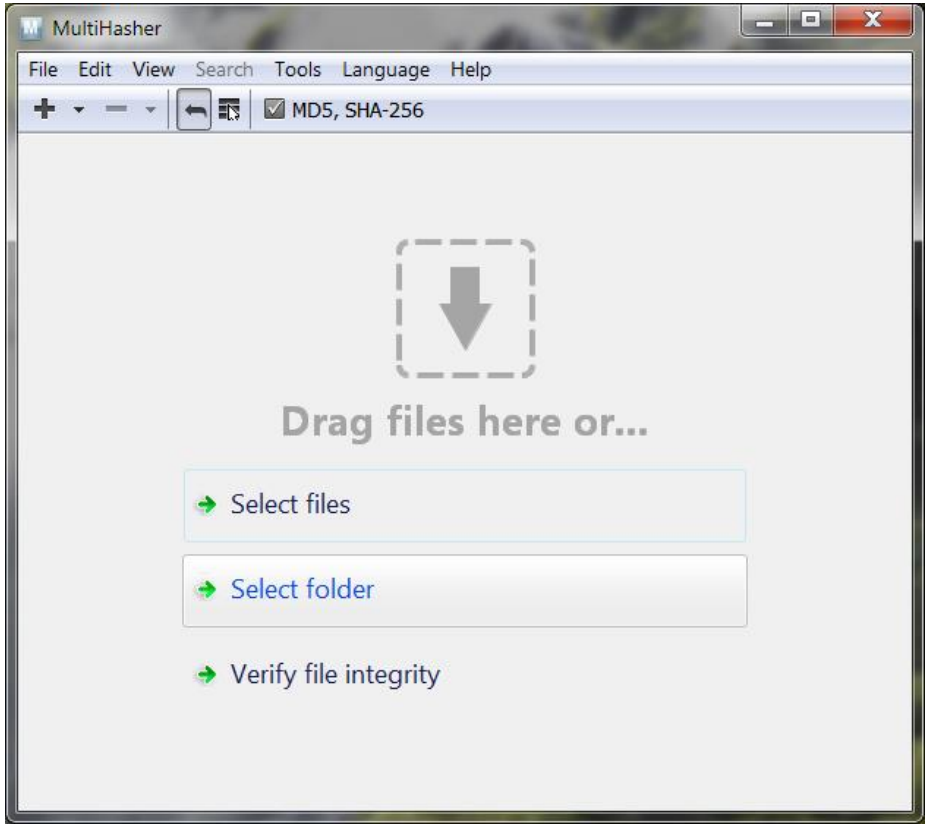
E.g: MD5 hash value of “Investigation.zip” located in the folder TEST:

certutil -hashfile C:\TEST\Investigation.zip MD5

E.g: SHA-256 hash value of “scan0006.jpg” located in the folder SMS Collect:

certutil -hashfile "C:\SMS Collect\scan0006.jpg" SHA256

BTSF Exercise: Calculating the hash code



Hashcalc

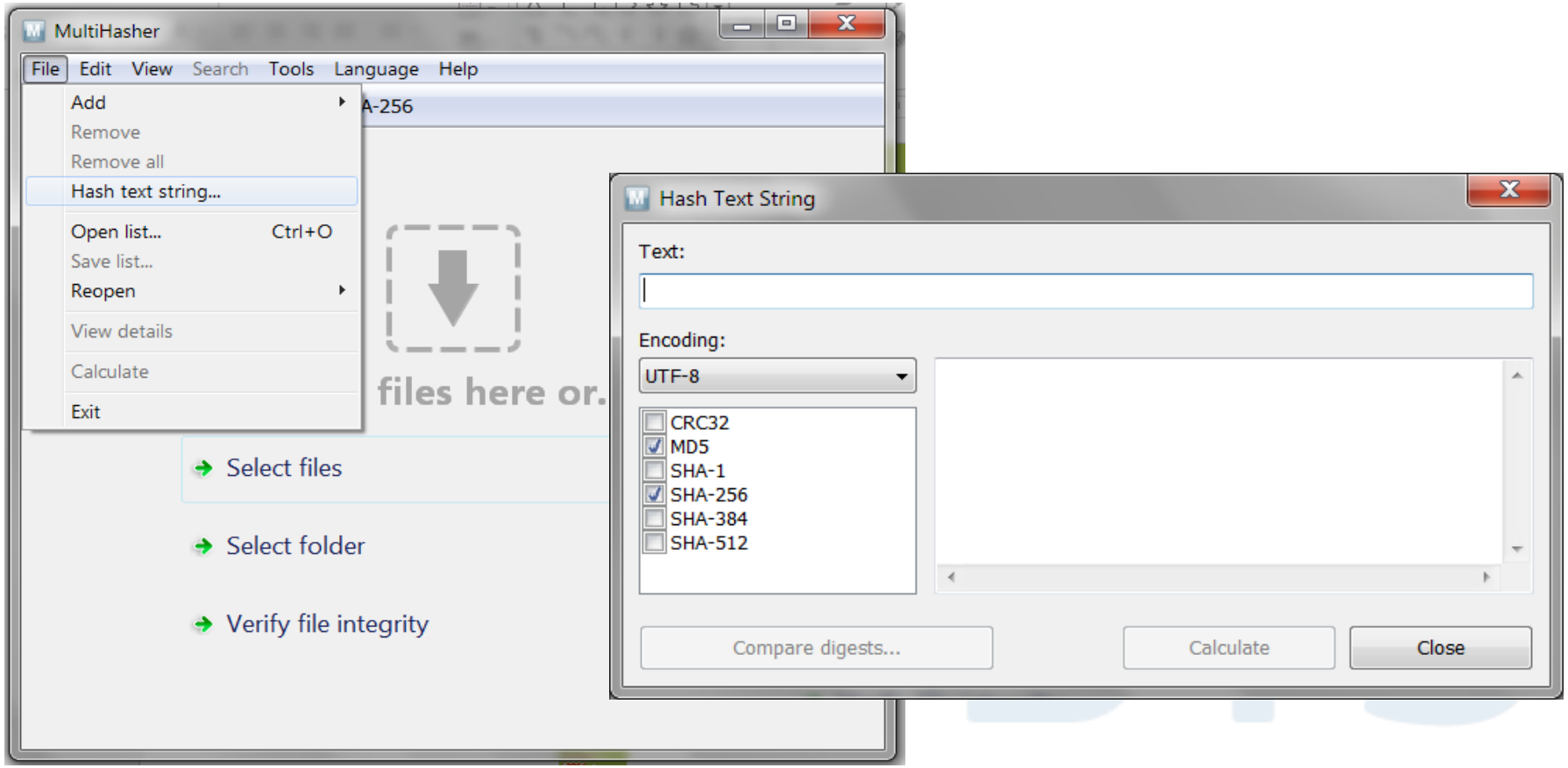
Multihasher

Karen's hasher

Win MD5

Quick Hash GUI

BTSF Exercise: Calculating the hash code

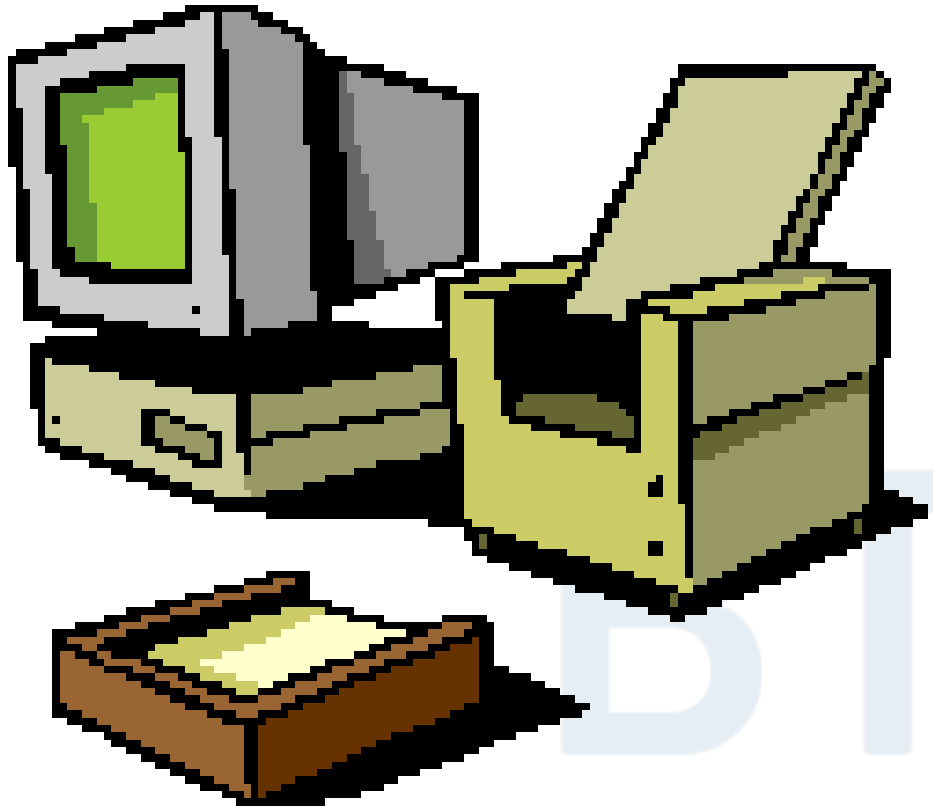


European Commission

BTSF Recording and reporting

- The identity of the investigator
- The date, time and place of the investigation
- The equipment and browser being used for each search
- Any special software being used
- The URL of the site visited and captured
- The way in which the website was captured
- The time of capturing and the reference number
- Hash value of each piece of evidence

BTSF Presenting Internet Evidence in document form

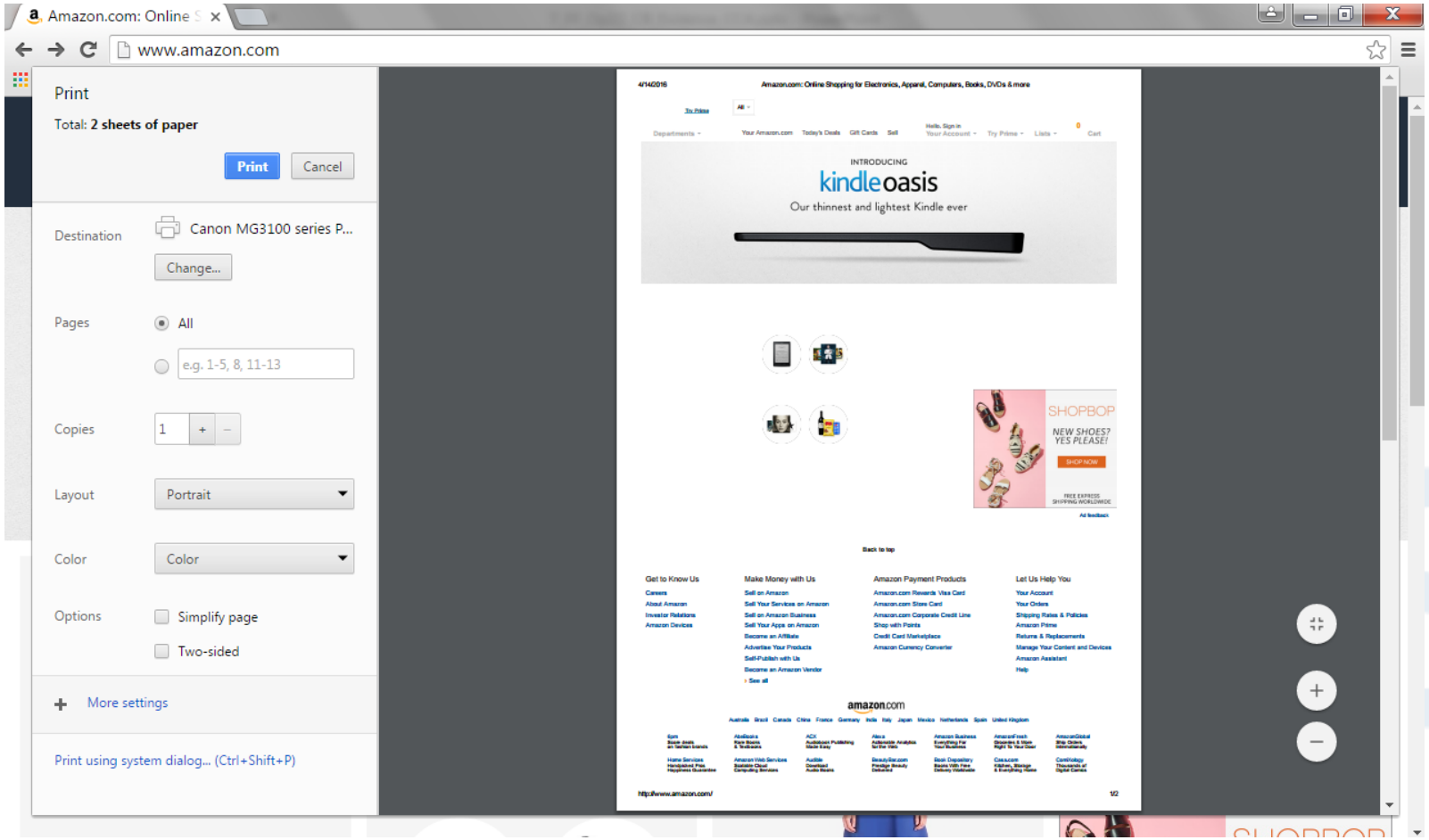


BTSF

Why paper?

- NOT for evidence – you have been warned!!
- Evidence must be collected and presented in native/original form
- Digital evidence
- Internal communication /presentations / training
- To assist third parties
- …Lawyers and Courts of Justice love paper

BTSF Browsers are poor at printing web pages



European Commission

BTSF

Alternatives

- Screenshot
- Screen grabing software
- Convert to PDF

BTSF

Alternatives

Static & Scrolling screenshot

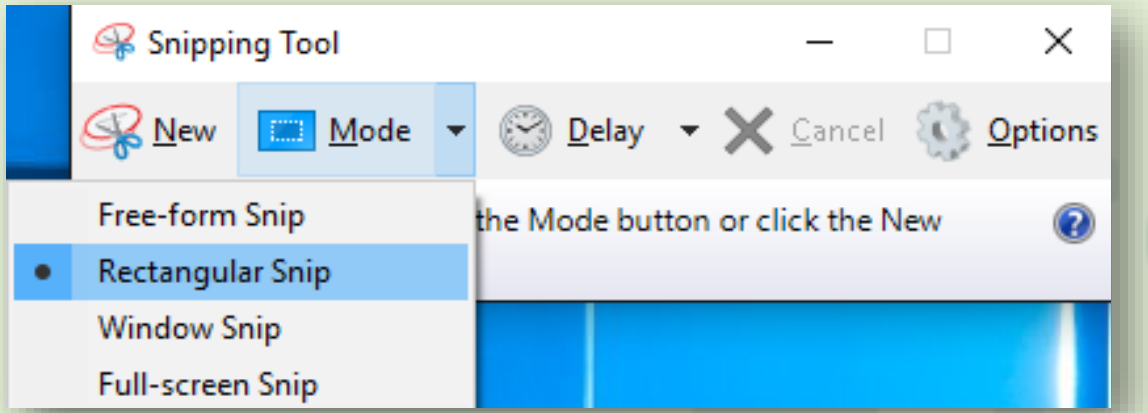
- Screenshots, also known as ‘screen grab’ or ‘screen capture’
- Like a photograph of what is displayed on your screen.
  - **Static screenshots** tools just capture what you see on the visible area of the browser window.
  - **Scrolling screen capture** tools can grab the information beneath the visible area, i.e. longer than the viewable screen.

BTSF

Alternatives

Operating system built-in features:

- Print Screen button
- Snipping Tool



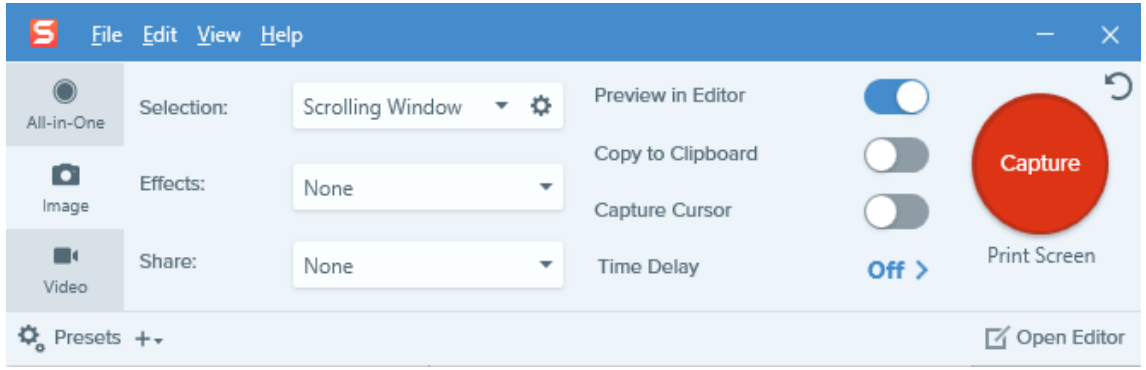
BTSF

Exercise: Creating static screen dumps of webpages

- Built into Windows
- Quick and easy
- Only captures what is on the screen
- Can be pasted into other documents
- Open the browser and go to any website
- Press “Alt” and “Prt Screen” together
- Open Paint application and paste in contents
- Save file to you evidence folder

BTSF Screen Grabbing Software

- Many software titles available (e.g. Snagit).

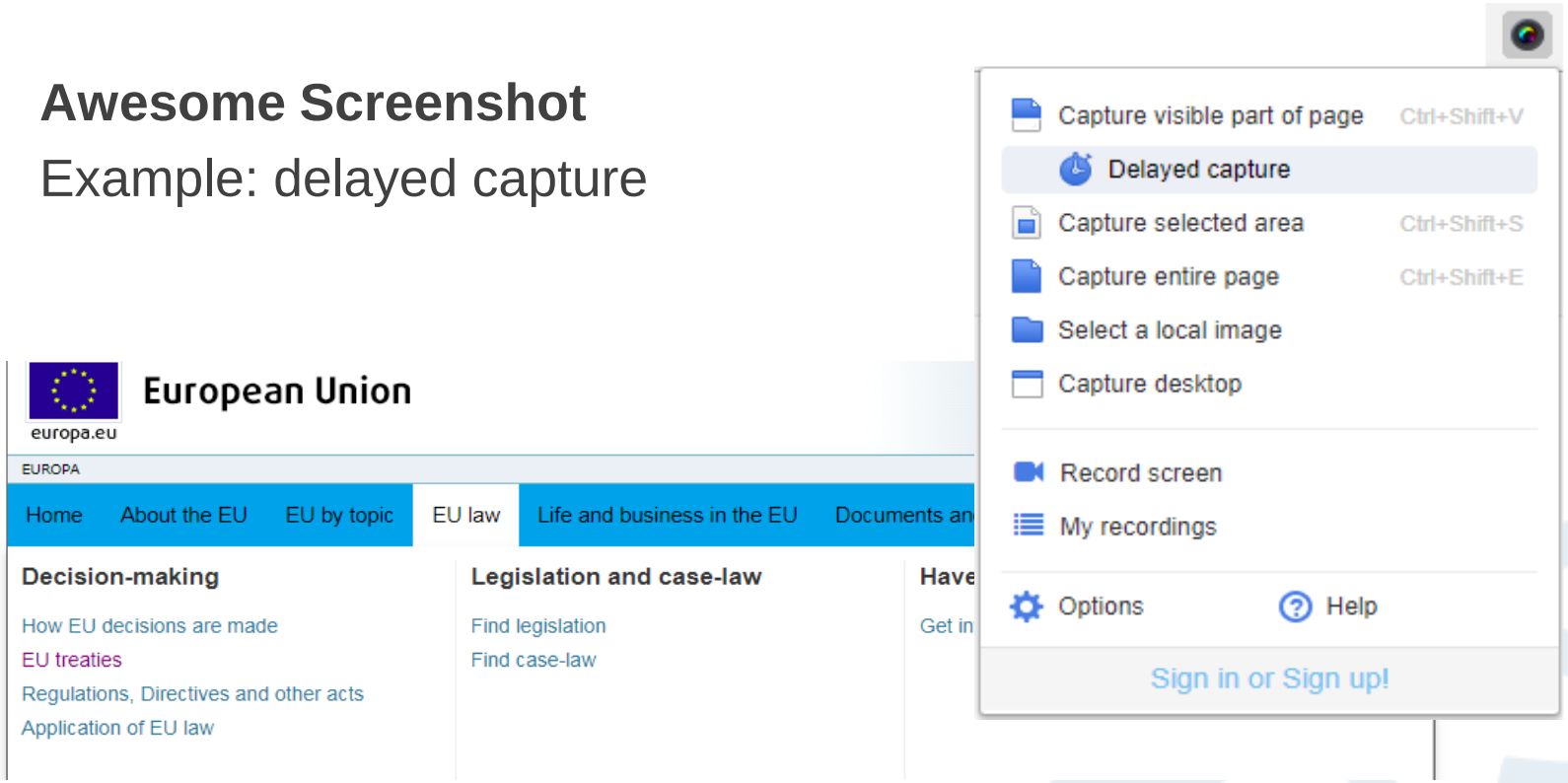


- Offer more flexibility than previous ones: e.g. capturing web pages longer than the screen.
- Results can be saved as jpg files or pasted into other documents such as reports in Microsoft Word.
- Web browsers have add-ons/extensions.

BTSF Example: Screen capture add-on for Firefox

Awesome Screenshot

Example: delayed capture

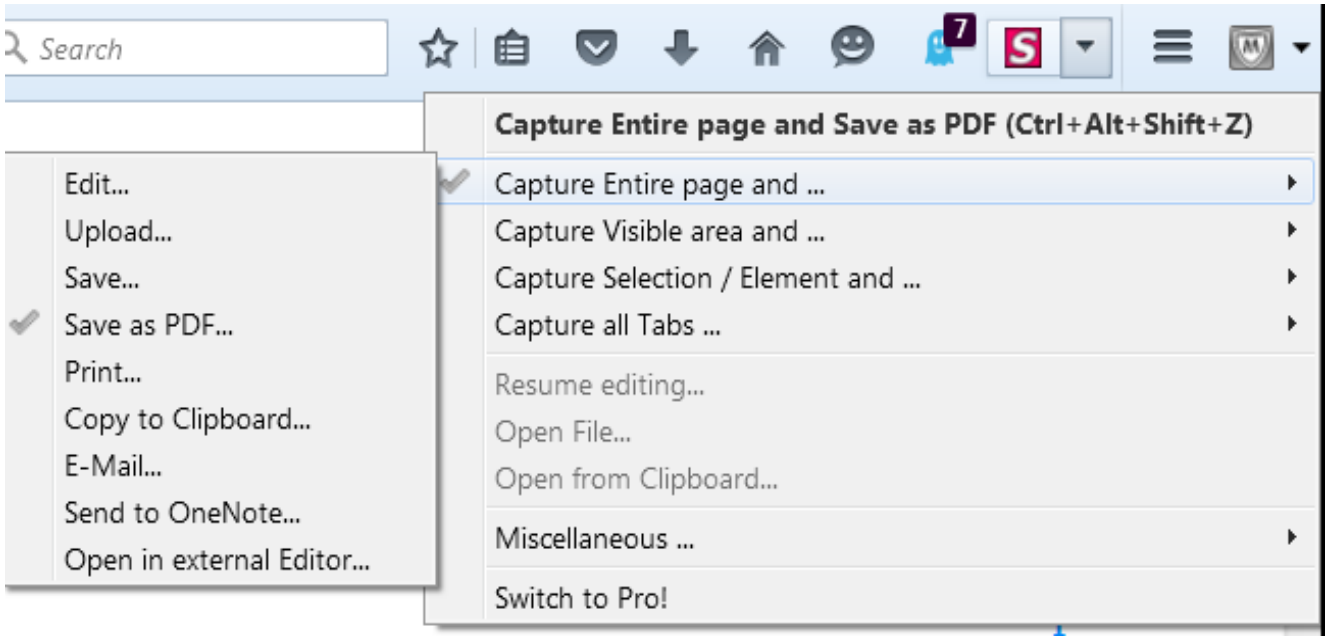


European Commission

BTSF Example: Screen capture add-on for Firefox

FireShot

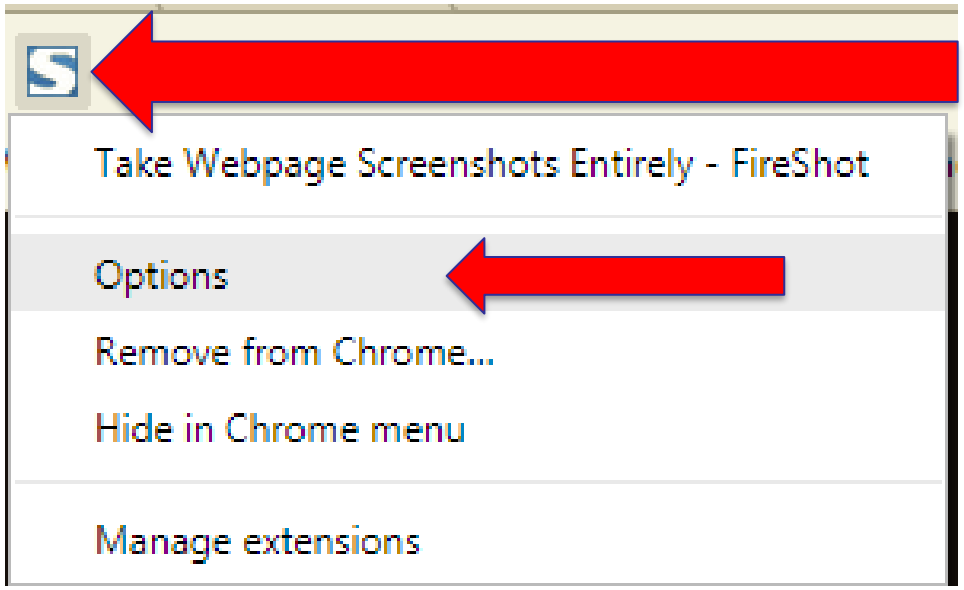
Example: capture entire page and save as pdf



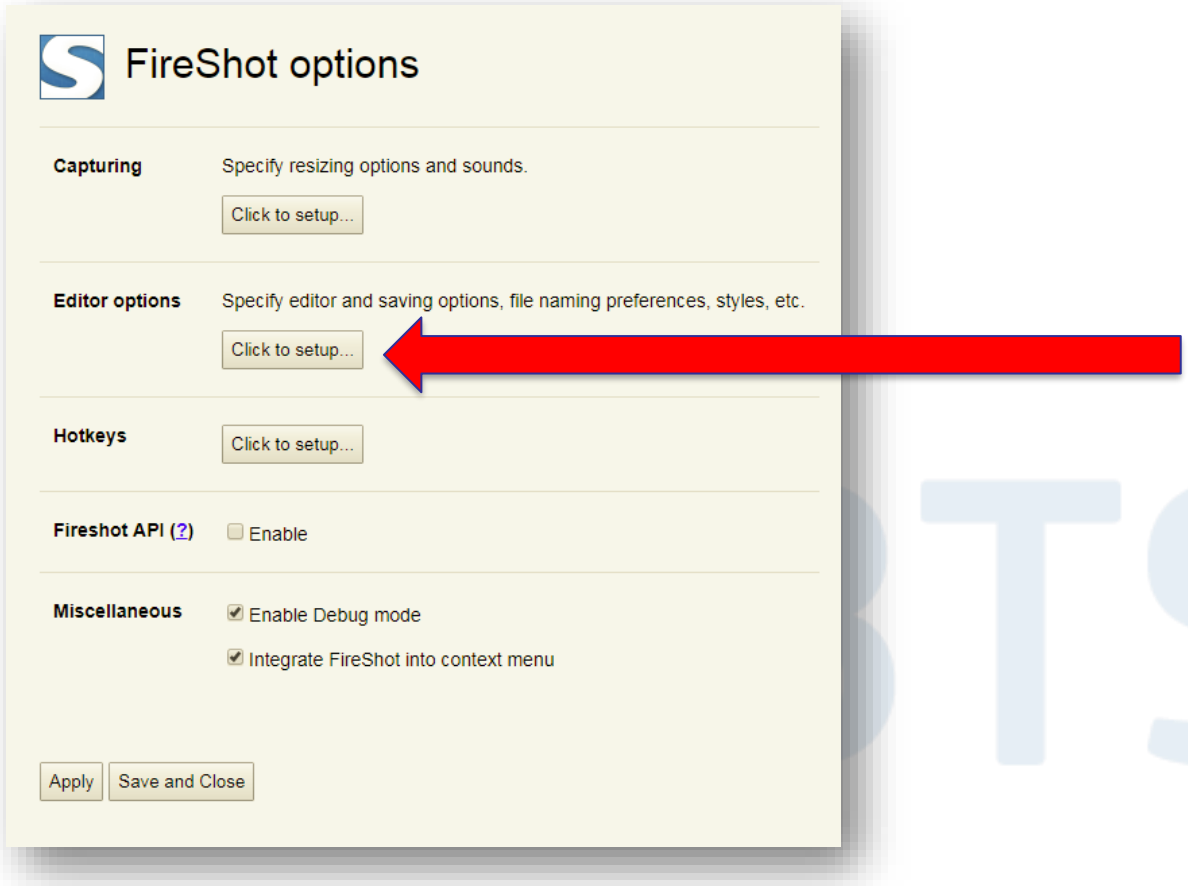
BTSF Example: Screen capture add-on for Firefox

FireShot (pro & trial-version)

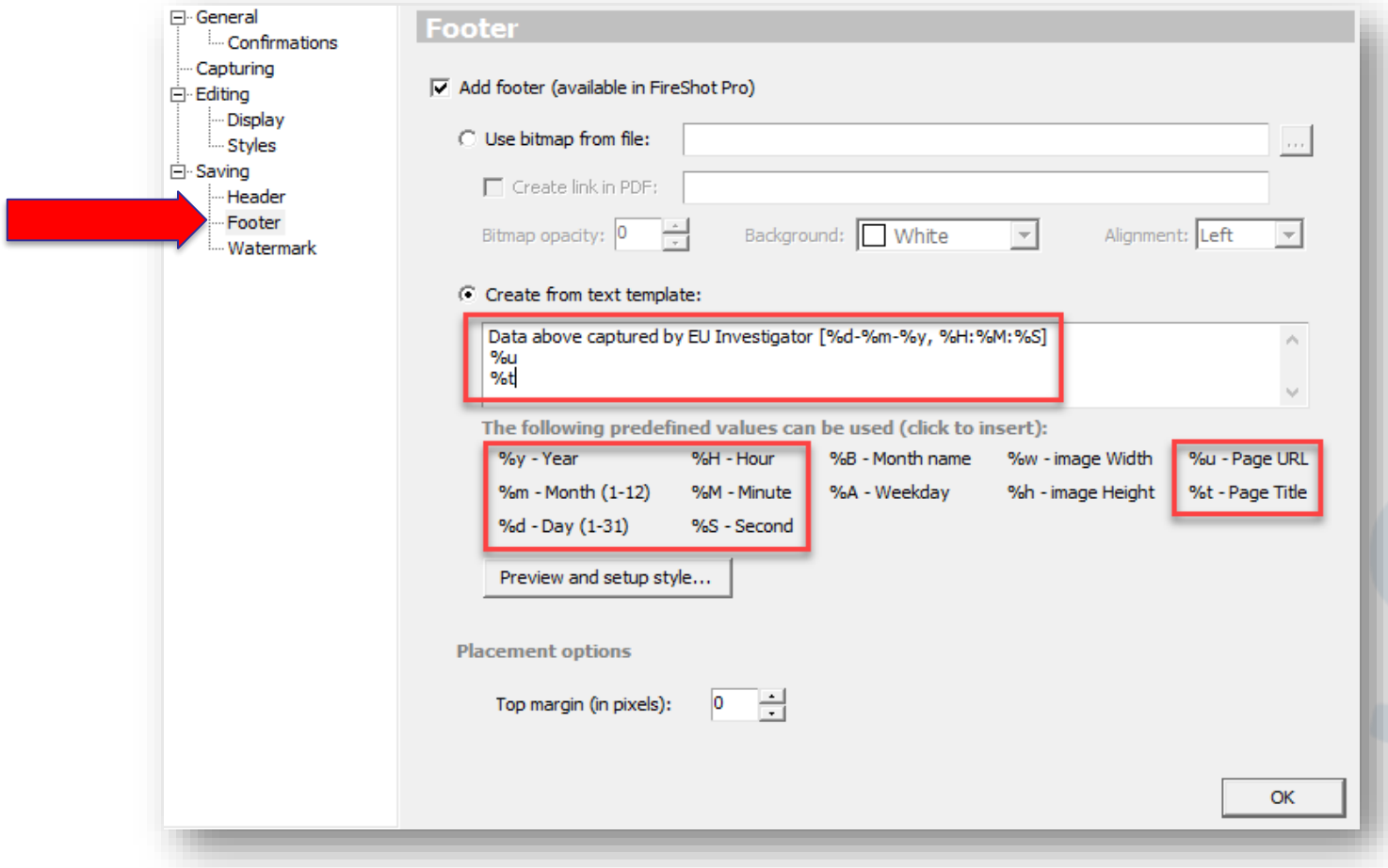
Example: automatic time-stamp



BTSF Example: Screen capture add-on for Firefox

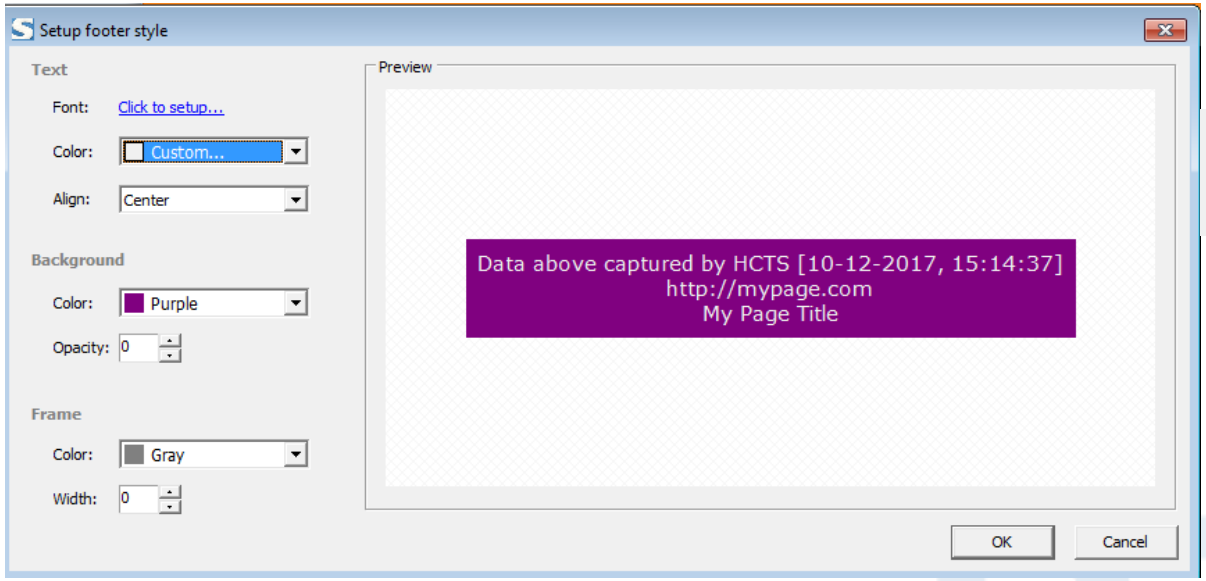


BTSF Example: Screen capture add-on for Firefox



European Commission

BTSF Example: Screen capture add-on for Firefox



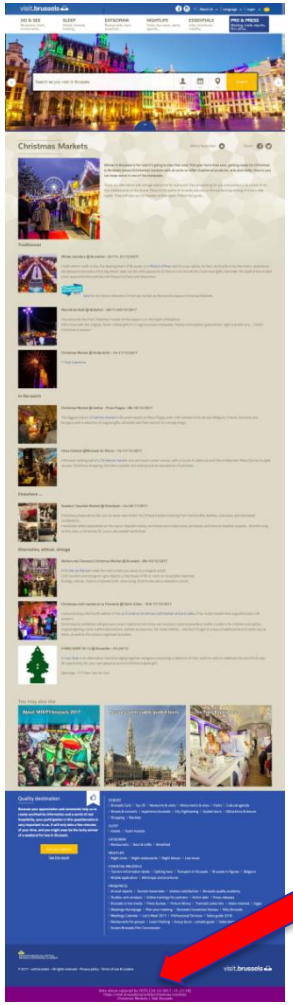
Preview and setup style...

Use a prominent colour to make the Footer stand out –separate from the data above the footer.

Data above captured by HCTS [10-12-2017, 15:14:37]
http://mypage.com
My Page Title

European Commission

BTSF Example: Screen capture add-on for Firefox



REGION DE BRUXELLES-CAPITALE
BRUSSELS HOOFDSTEDELIJK GEWEST

© 2017 - visit.brussels - All rights reserved - Privacy policy - Terms of use & Cookies

visit.brussels

Data above captured by HCTS [10-12-2017, 15:23:18]
https://visit.brussels/en/article/christmas-markets
Christmas Markets | Visit Brussels

Note: Links in Footer are click-able

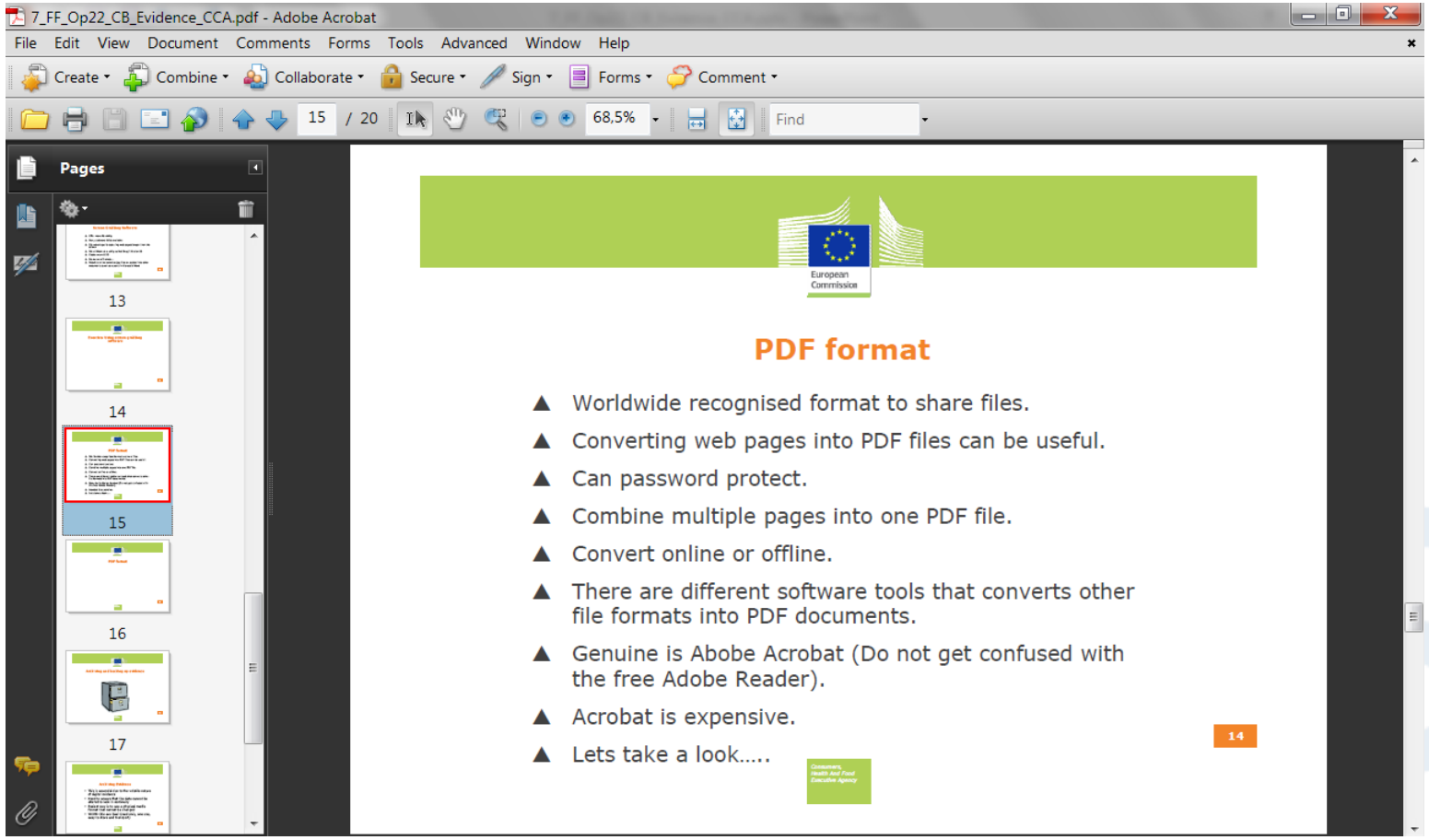
Data above captured
https://visit.brussels/en/article/christmas-markets
https://visit.brussels/en/article/christmas-markets
Christmas Markets | Visit Brussels

European Commission

BTSF PDF format

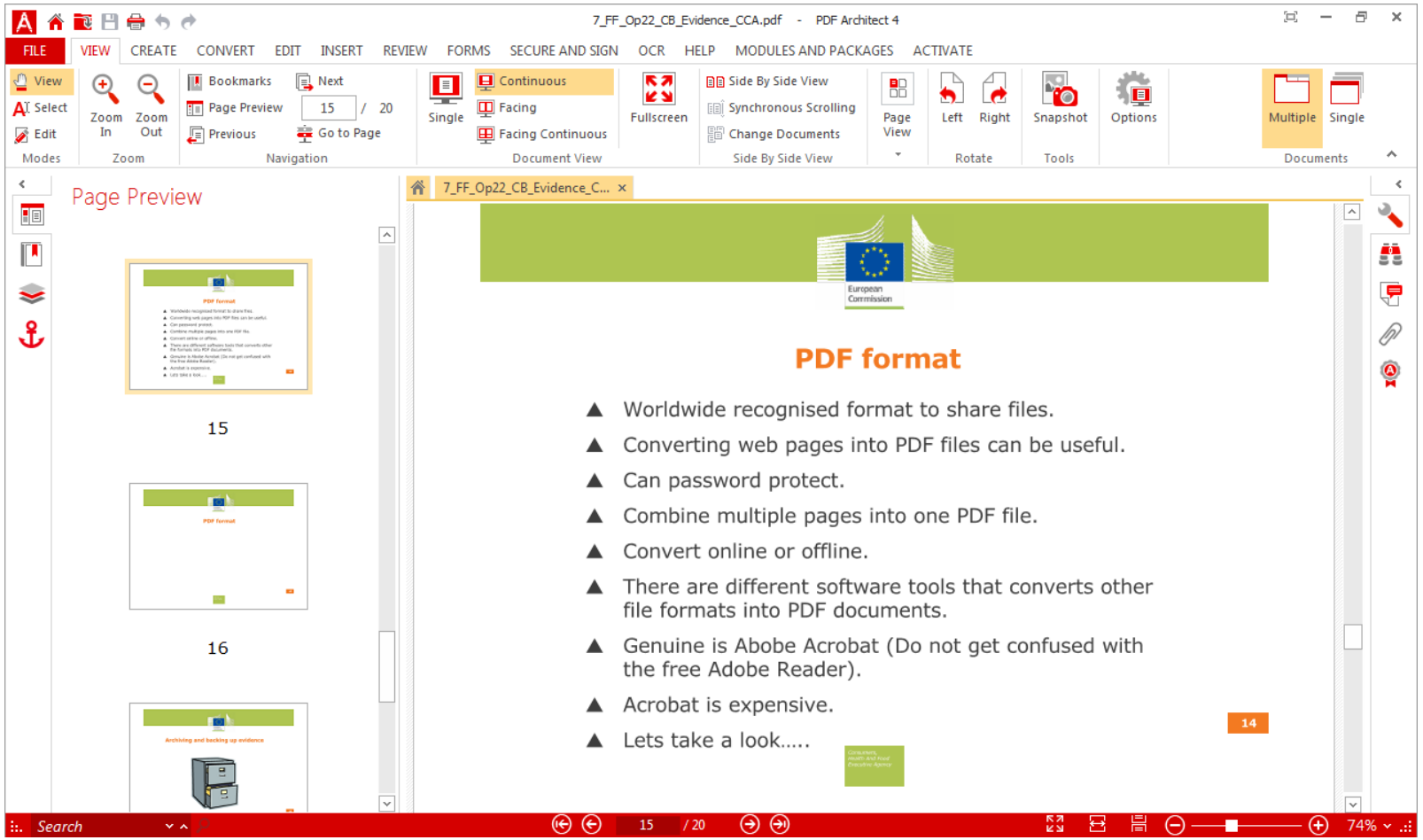
- Worldwide recognised format to share files.
- Converting web pages into PDF files can be useful.
- Can password protect.
- Combine multiple pages into one PDF file.
- Convert online or offline.
- There are different software tools that converts other file formats into PDF documents.
- Genuine is Adobe Acrobat (Do not get confused with the free Adobe Reader).
- Acrobat is expensive.

BTSF Adobe Acrobat



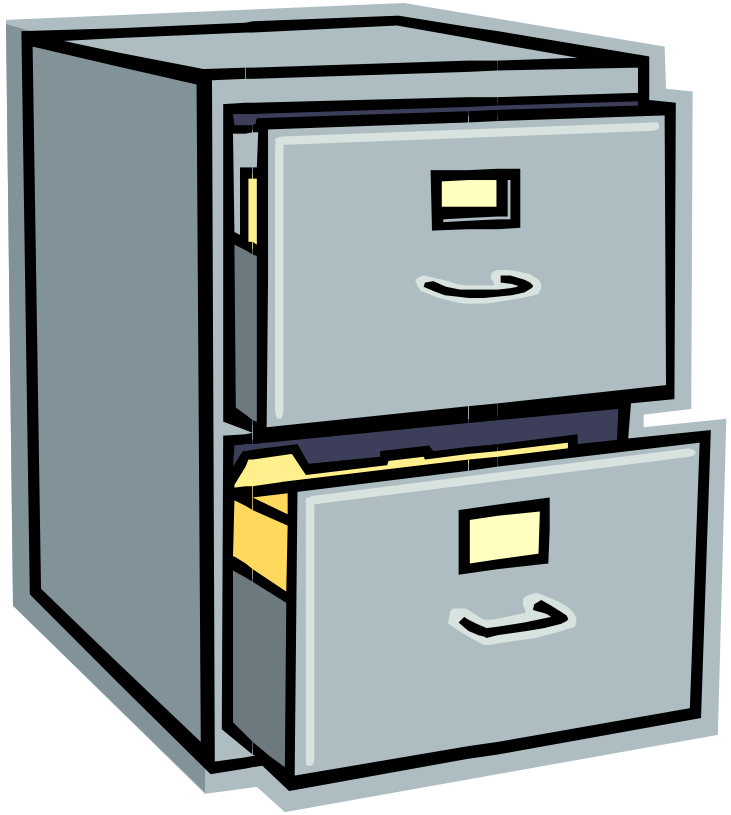
European Commission

BTSF PDF Architect



European Commission

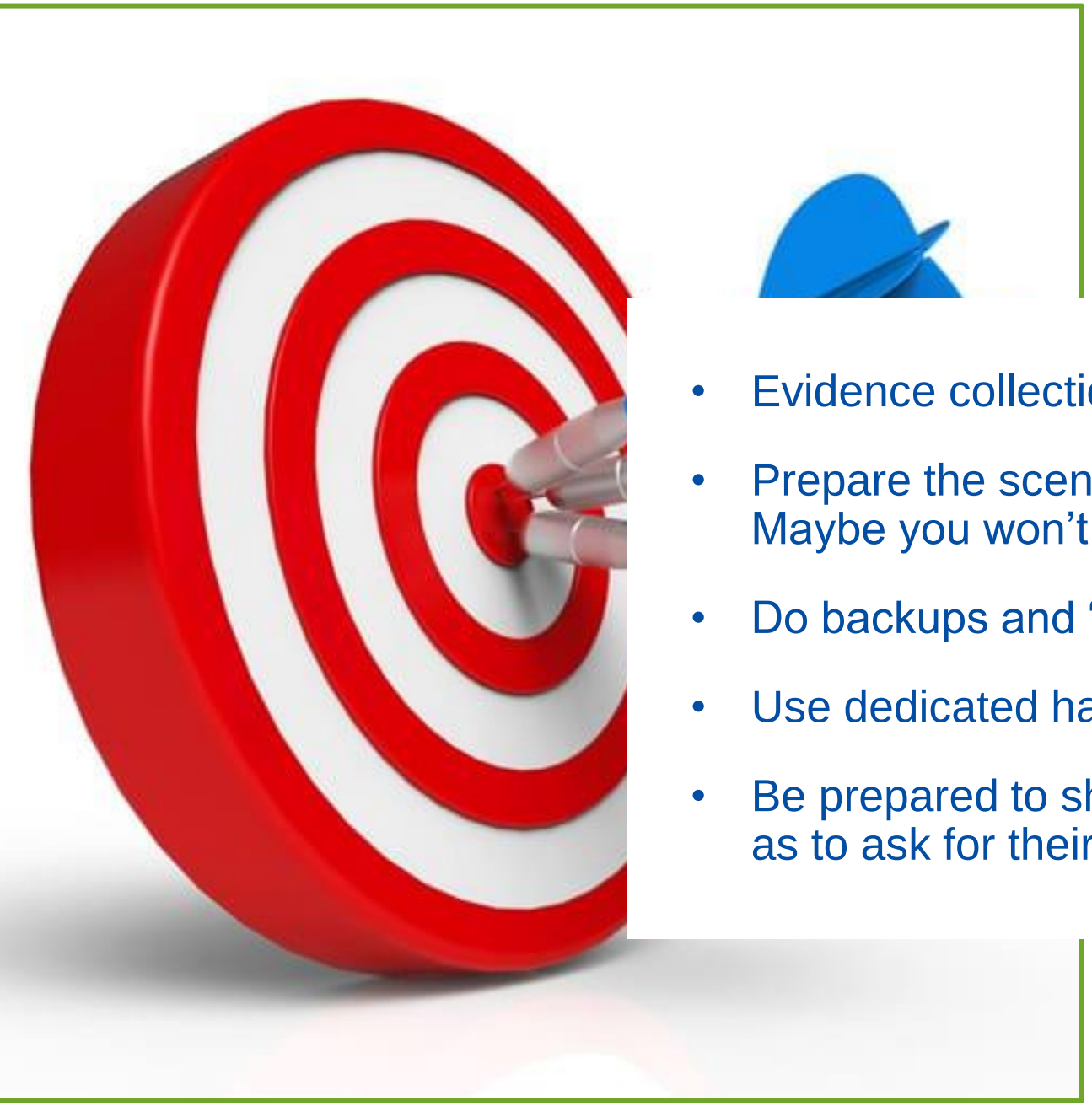
BTSF Archiving and backing up evidence



BTSF

Archiving Evidence

- This is essential due to the volatile nature of digital evidence.
- Need to ensure that the data cannot be altered to lock in continuity.
- Easiest way is to use a physical media format that cannot be changed.
- Although out of fashion, WORM (Write once read many) CDs/DVDs are useful (read only, one use, easy to store and transport).
- Operating system built-in feature and other software.



BTSF

Things to remember

- Evidence collection must be traceable and well documented.
- Prepare the scenario (time, place, parties, tools, forms, etc.). Maybe you won’t have more opportunities…
- Do backups and “freeze” evidence in its original format.
- Use dedicated hardware and software during investigations.
- Be prepared to share your data with other investigators as well as to ask for their cooperation

BTSF

Thank you

European Commission
Consumers, Health and Food Executive Agency
DRB A3/042
L-2920 Luxembourg

AENOR INTERNACIONAL
6, Genova street. 28004. Madrid, SPAIN
Tel: +34 91 432 61 25
Mail: 20179605NFIT@aenor.com
www.btsf-aenor.com

European Commission