



Teaching Cyber Forensics in the Covid Era

Stuart Richards

About Me



- 17 Yrs Providing electronic security and surveillance systems for HMG, Military, High Value /Risk target in UK and abroad
- 10 years with Gwent / SW Police JSIU
 - Msc Computer Forensics USW
 - Lead Mobile Device Examiner
- Private Sector (contract work for Police)
- UOG Academic course Leader 4Years

Traditional Module Delivery

- Hi to the students
- Set out the aims for today
- Everybody Logs in !!
- I'm there to help
- Student Assistants are there to help

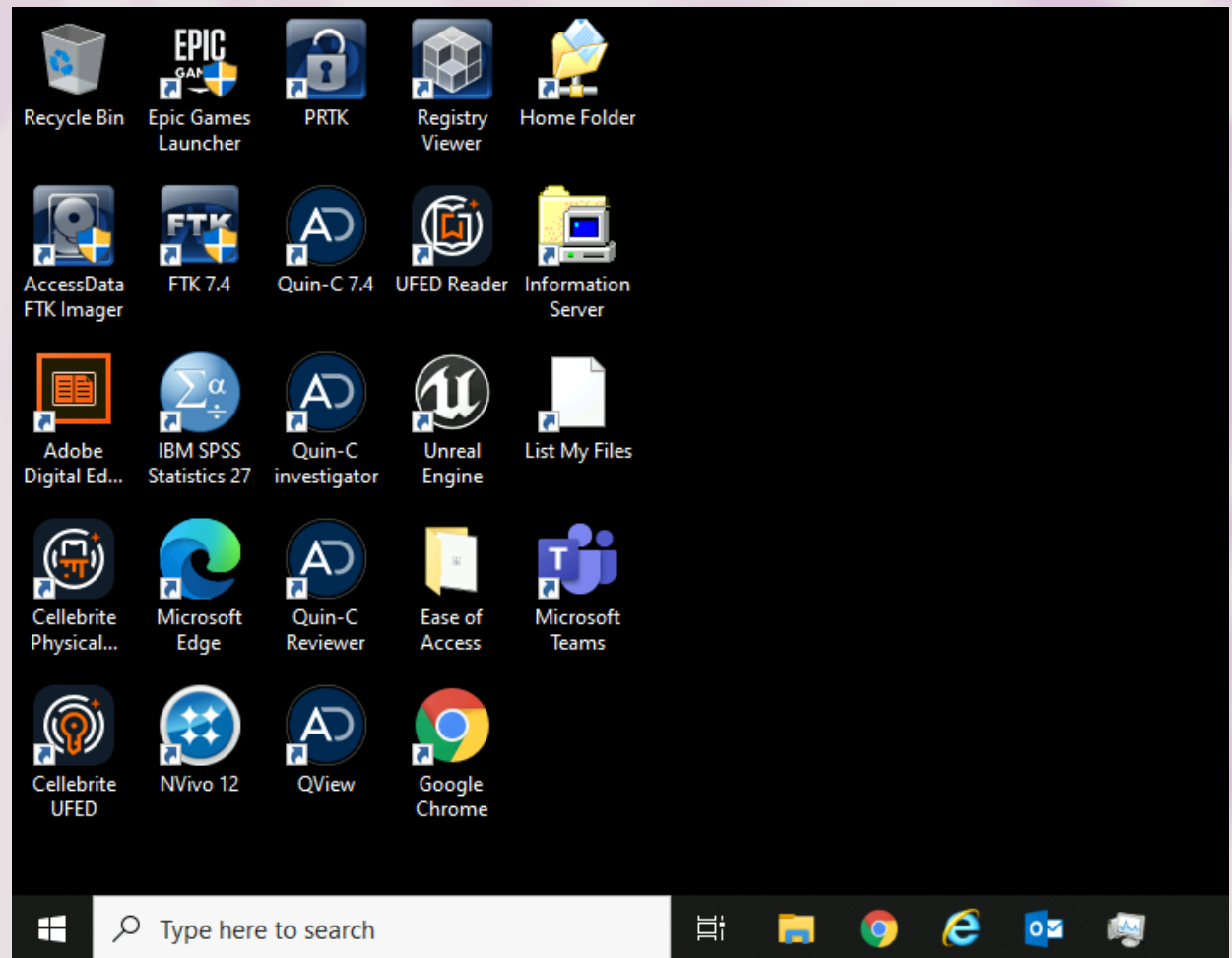


Work through the Session

- Looking over their shoulders.
- Sharing successes and failures
- Those little conversations that lead to a crucial learning point (something that can never be planned)
- Strong students help the ones who won't ask.

It's all in place

- The labs work (fingers crossed!!)
- Problems can be sorted immediately
- Physical objects to work with
 - USB to Image etc
 - Phones to plug in (and break)
- Share the Kit
 - Cables ,write blocker ,etc



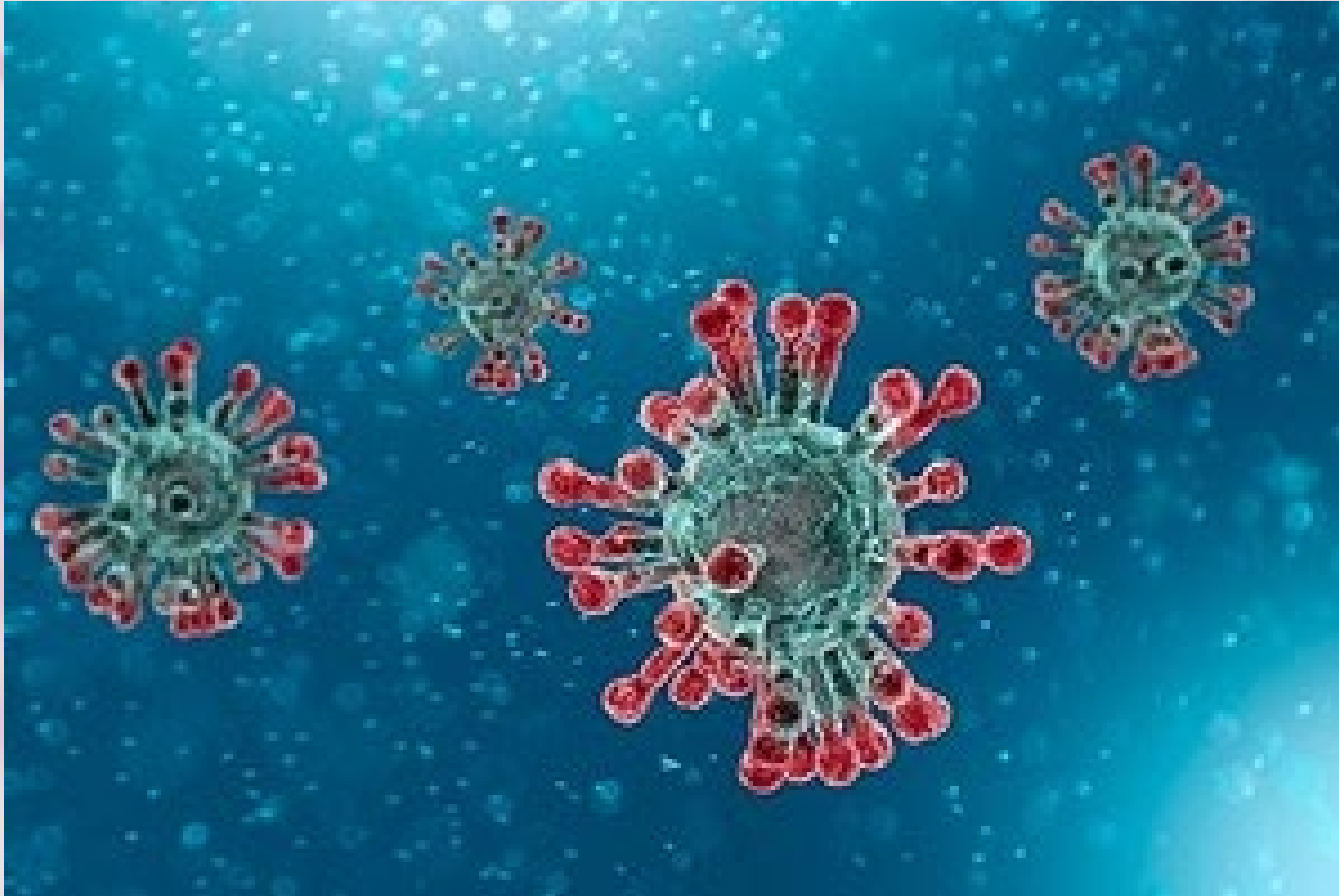
“That Student”

- Every course has one.
- Knows their stuff
- Helps the others
- Encourages conversations
- Is a pain in the neck - But in a good way

When it's Over

- Questions from the group.
- Shared experience of answers
- The shy student
- The struggling student
- Study buddies
- Direct feedback from the room (how did it feel?)





Teaching in the Covid Era.

Internet poverty

- Lack of suitable equipment (only have a Mac)
- Not the only one using the connection
- Siblings , Children, Noisy environment

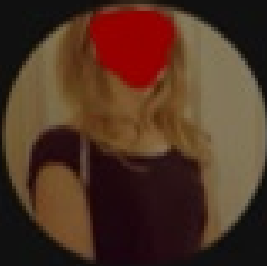
Notes on the gentle art of herding cats

1. Cats don't like to be herded
(in fact, you can't really herd cats)
2. Cats prefer to herd themselves
3. Cats understand that they sometimes need to be herded (that doesn't make them any easier to herd)
4. Cats don't like being reminded that they are being herded
5. Harsh herding has negative consequences





Where is the personal touch?



This afternoon we're gonna look

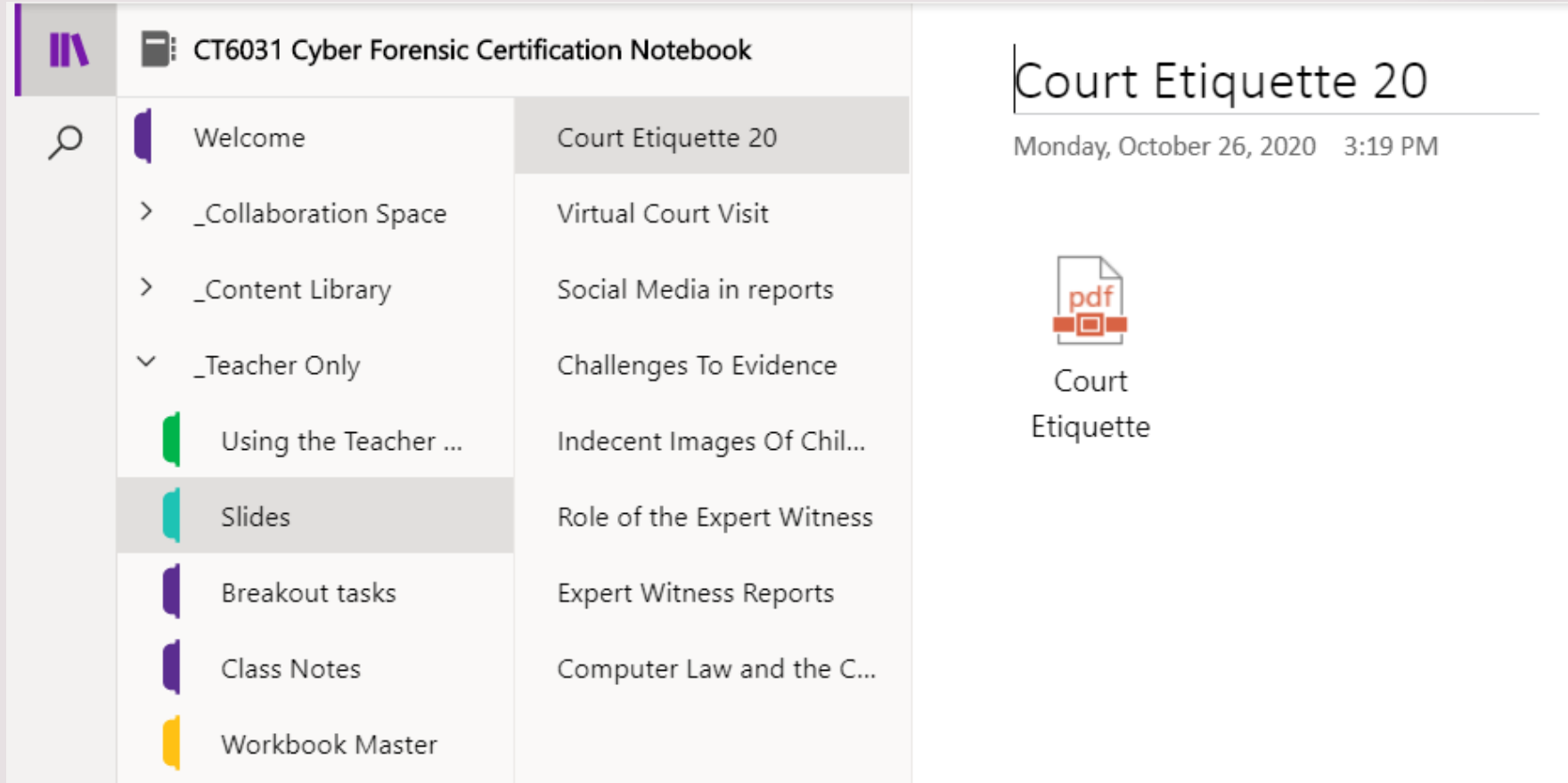
Delivery Methods

Teams

- Easy to control
- Easy to update content
- Messaging
- Chat for students
- Breakout rooms for discussions



Teams as a Work Environment



The screenshot displays a Microsoft Teams channel interface. The channel name is "CT6031 Cyber Forensic Certification Notebook". The left-hand navigation pane shows a search icon and a list of items: "Welcome", "_Collaboration Space", "_Content Library", "_Teacher Only", "Using the Teacher ...", "Slides", "Breakout tasks", "Class Notes", and "Workbook Master". The "Slides" item is currently selected. The main content area shows the title "Court Etiquette 20" with a timestamp of "Monday, October 26, 2020 3:19 PM". Below the title is a PDF icon and the text "Court Etiquette".

Navigation Pane	Channel Content
Welcome	Court Etiquette 20
> _Collaboration Space	Virtual Court Visit
> _Content Library	Social Media in reports
∨ _Teacher Only	Challenges To Evidence
Using the Teacher ...	Indecent Images Of Chil...
Slides	Role of the Expert Witness
Breakout tasks	Expert Witness Reports
Class Notes	Computer Law and the C...
Workbook Master	

Practical problems of remote delivery

- Large Data sets
- Physical Kit required



Software

- Not just a question of downloading.
- Activation dongles held on local server
- Remote licence very expensive
- How to control unauthorised use?

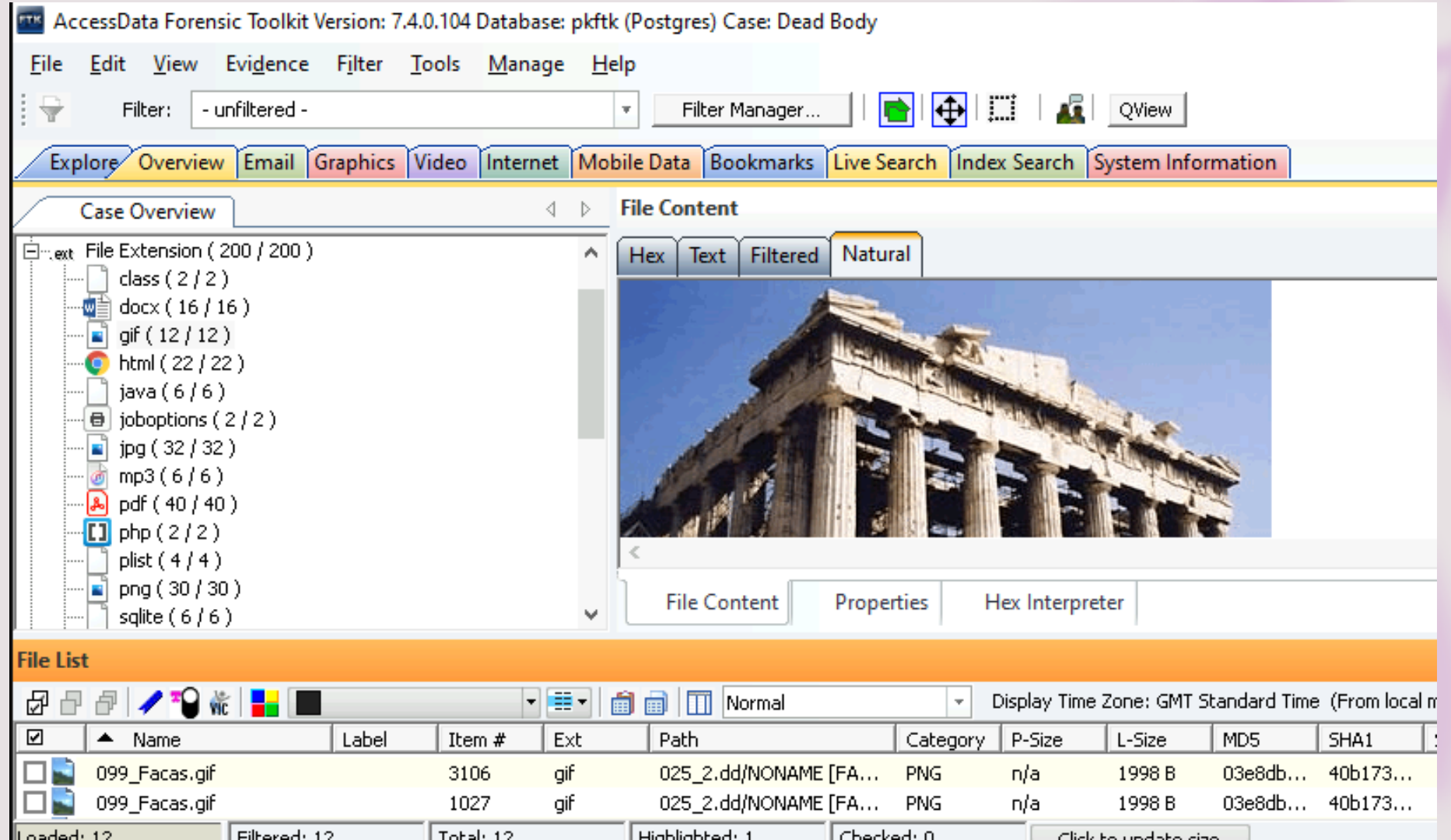
Crime Scene Module



- How do you deliver a physical search experience remotely ?

Enough of the doom and gloom

Let's see what works



AccessData Forensic Toolkit Version: 7.4.0.104 Database: pkftk (Postgres) Case: Dead Body

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Video Internet Mobile Data Bookmarks Live Search Index Search System Information

Case Overview File Content

Hex Text Filtered Natural

File Extension (200 / 200)

- class (2 / 2)
- docx (16 / 16)
- gif (12 / 12)
- html (22 / 22)
- java (6 / 6)
- joboptions (2 / 2)
- jpg (32 / 32)
- mp3 (6 / 6)
- pdf (40 / 40)
- php (2 / 2)
- plist (4 / 4)
- png (30 / 30)
- sqlite (6 / 6)

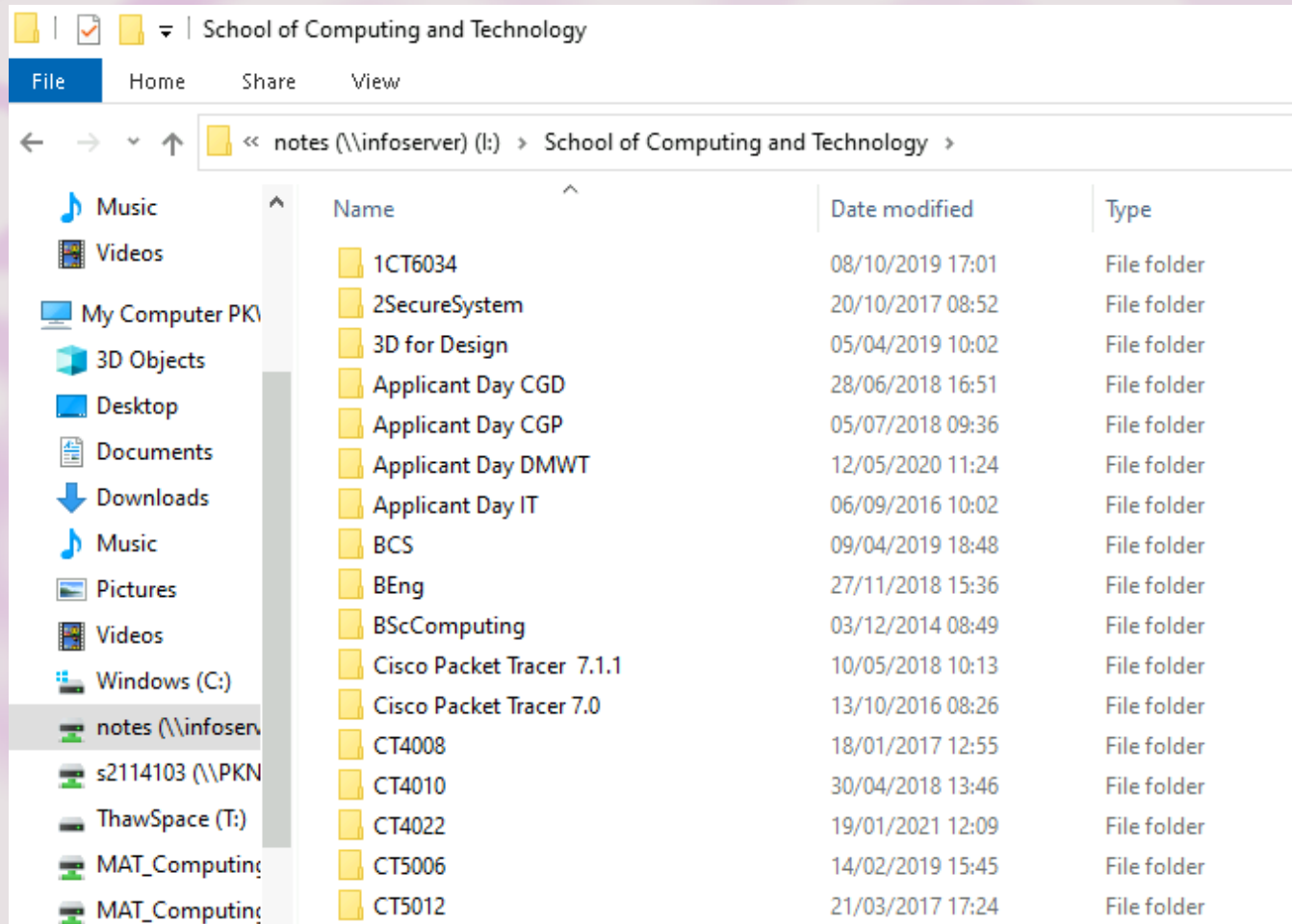
File Content Properties Hex Interpreter

File List

Normal Display Time Zone: GMT Standard Time (From local m

<input checked="" type="checkbox"/>	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1
<input type="checkbox"/>	099_Facas.gif		3106	gif	025_2.dd/NONAME [FA...	PNG	n/a	1998 B	03e8db...	40b173...
<input type="checkbox"/>	099_Facas.gif		1027	gif	025_2.dd/NONAME [FA...	PNG	n/a	1998 B	03e8db...	40b173...

Loaded: 12 Filtered: 12 Total: 12 Highlighted: 1 Checked: 0 Click to update size



Data sets on Uni drive

Scenario based assignments

- Assignment 2
- Operation Gorgon
 - Following an undercover investigation into an “Eco - Terrorist” cell a USB device has been recovered from the home address of one of the lead suspects. An informant has already provided details of an imminent attack on 5G infrastructure in the UK.
 - Your task is to recover any usable evidence from the device and provide information to corroborate details already uncovered.
 - USB to contain details of
 - 1 Location of attack
 - 2 Images of bombs
 - 3 Details of vehicles used
 - 4 Documents detailing previous attacks
 - 5 Contact details for cell.

Workgroups/Teams

- Work well over MS Teams
- Student mutual support
- Common questions / answers (only one point of contact)
- Get used to working with staff in deferent areas.
- Enhances communication skills
- Enhances employability skills
- Remote working is here to stay.

Students lead the development of new methods

- Feedback is essential
- What works?
- What doesn't
- What do employers want?/ say?
- Share best practices

IMPROVISE

ADAPT

OVERCOME

Thank You!

Any Questions?

srichards5@glos.ac.uk